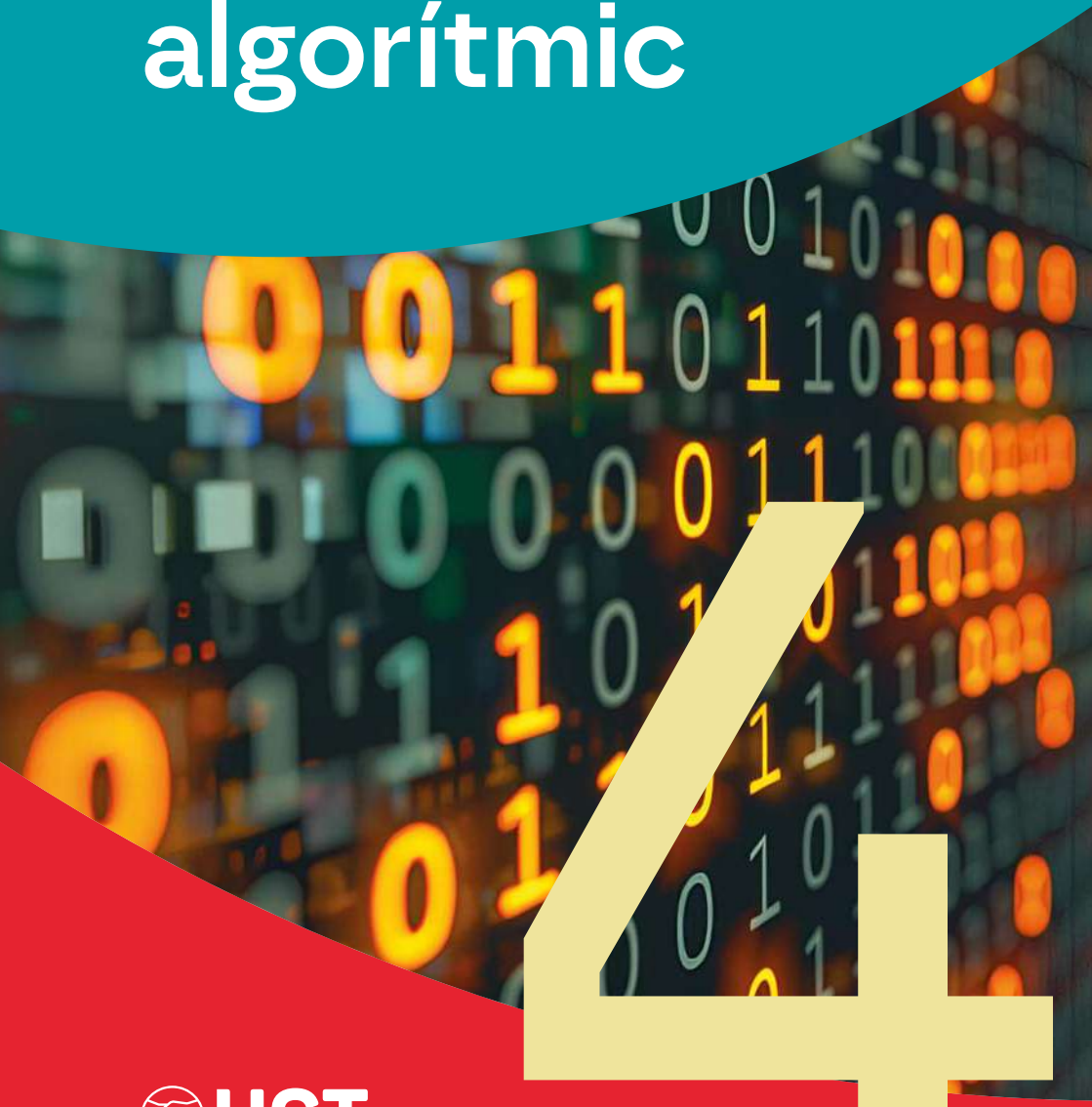
Guia de drets laborals i de prevenció de riscos: IA i vigilància tecnològica

Control algorítmic



4

UGT.cat

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

Control algorítmic

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 11744-2026

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

Control algorítmic

4

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.

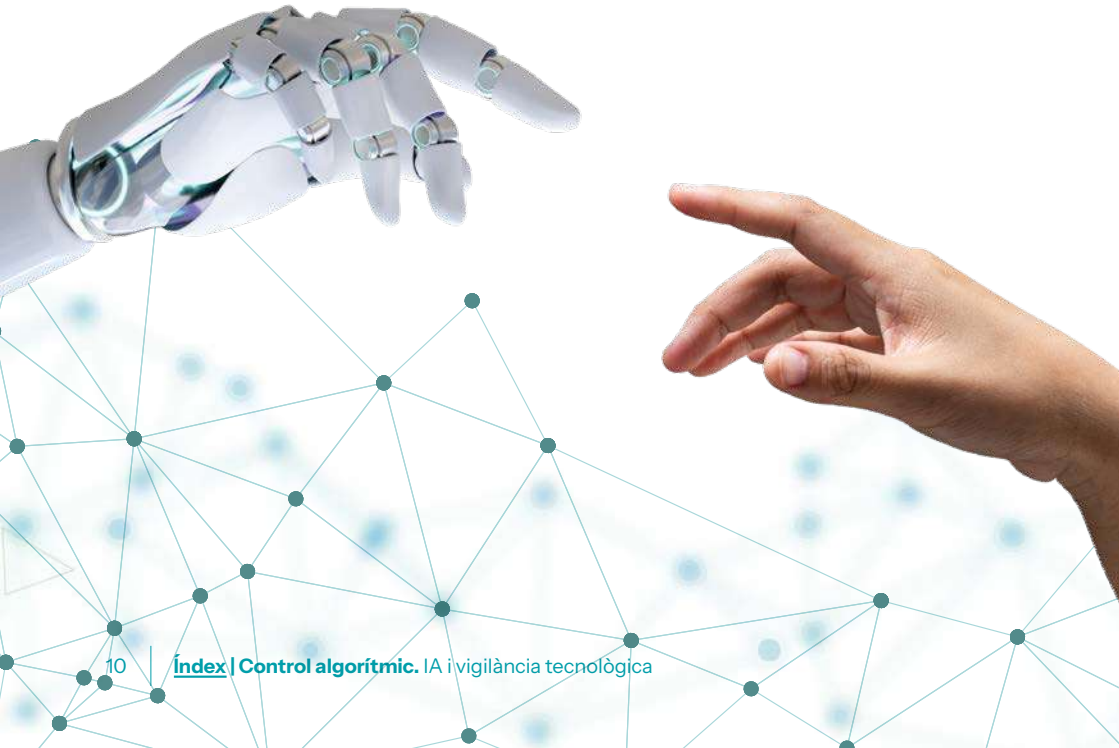
Davant aquest escenari, l'**acció sindical** és imprescindible. La defensa dels drets laborals en l'era digital no pot quedar limitada a l'aplicació mínima de la normativa existent. Cal una intervenció activa, informada i estratègica per part dels sindicats, especialment en l'àmbit de la **negociació 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 control algorítmic

Poden ser utilitzats sistemes algorítmics per controlar les persones treballadores?

Els sistemes algorítmics són conjunts ordenats d'operacions matemàtiques capaços de processar grans volums de dades per resoldre problemes o adoptar decisions. El seu principal tret és l'habilitat per recopilar i tractar quantitats massives de dades a gran velocitat. En l'àmbit laboral, aquestes tecnologies poden ser utilitzades per recopilar dades, processar-les i prendre decisions sobre múltiples aspectes de la relació de treball (p. ex., selecció de personal, avaluació i direcció de les persones treballadores, distribució de tasques, etc.). Amb aquests sistemes, l'empresa pot analitzar informació relativa al rendiment, el comportament o fins i tot l'estat físic de la persona treballadora, generant indicadors de productivitat o rànquings interns de rendiment que poden influir directament en les condicions laborals (p. ex., en l'aplicació de sancions, en la distribució d'horaris, etc.). Les dades poden ser obtingudes de diferents fonts: sensors, rellotges intel·ligents, escàners, anàlisi de xarxes socials, xips, targetes magnètiques, controls biomètrics, seguiment de correus electrònics, etc.

Aquests sistemes presenten, a més, característiques rellevants des de la perspectiva jurídica:

1. Poden tractar dades personals, sovint de naturalesa especialment sensible (com les dades de salut); quan s'empren, per exemple, *wearable devices* (rellotges o polseres intel·ligents) que analitzen les pulsacions de les persones treballadores o sistemes de reconeixement

d'emocions que identifiquen si la persona treballadora està alegre, trista, indignada, etc.

2. Permeten l'adopció de decisions automatitzades, és a dir, decisions en les quals no existeix una intervenció humana significativa, que poden incidir en la selecció, l'assignació de tasques, la fixació de salaris, les promocions o els acomiadaments.

3. Poden integrar intel·ligència artificial, cosa que els permet aprendre de la informació analitzada, identificar patrons i automatitzar processos complexos.

4. Solen combinar-se amb tecnologies com la videovigilància, la geolocalització o els propis dispositius digitals facilitats a la persona treballadora.

Per això, la seva utilització requereix atendre tant les obligacions derivades del Reglament General de Protecció de Dades i la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, com del Reglament d'Intel·ligència Artificial.

En definitiva, els sistemes algorítmics poden emprar-se en l'àmbit laboral per monitorar l'activitat laboral i facilitar la presa de decisions. No obstant això, el seu ús implica un control molt més exhaustiu i permanent sobre el rendiment i el comportament de les persones treballadores. Això pot suposar una major ingerència en els drets fonamentals de les persones treballadores, com el dret a la intimitat, a la protecció de dades, a la no discriminació o a la integritat física i moral, la qual cosa exigeix valorar en la seva implementació si es compleixen les garanties legalment recollides i el principi de proporcionalitat.

Quins sistemes de control algorítmic estan prohibits per la normativa?

Els sistemes algorítmics utilitzats per supervisar l'activitat laboral permeten exercir un control més exhaustiu i continu sobre les persones treballadores. La potencial incidència d'aquestes eines en els seus drets fonamentals ha conduït el poder legislatiu a prohibir determinats usos, funcions o capacitats que poden integrar-se en aquest tipus de sistemes:

1. Gravació de sons

La Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals prohibeix l'ús de sistemes de gravació de sons en el lloc de treball, excepte per raons de seguretat. Per això, els sistemes de control algorítmic no podran incorporar tecnologies de gravació de sons.

2. Tractament de categories especials de dades

El Reglament General de Protecció de Dades (RGPD) prohibeix el tractament de dades especialment sensibles (com les dades biomètriques dirigides a identificar una persona o les dades de salut). L'empresa només podrà utilitzar aquesta tipologia de dades per dur a terme el control algorítmic 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, etc.).

3. Presa de decisions individuals automatitzades

Les decisions individuals automatitzades (p. ex., si el sistema detecta que la persona treballadora no es troba en moviment i envia directament un missatge indicant que cal continuar amb l'activitat laboral), inclosa l'elaboració de perfils, que es nodreixen de dades personals, estan prohibides quan produeixen efectes jurídics en la persona objecte de la decisió o l'afecten significativament (art. 22.1 RGPD). Tanmateix, aquesta prohibició s'alça en aquells supòsits en què la decisió és necessària per a la formalització o l'execució d'un contracte entre la persona interessada i la persona responsable del tractament (art. 22.2.a) RGPD), com podria ser-ho un contracte de treball. Si s'acredita el caràcter necessari de la decisió automatitzada (p. ex., una activitat no pot ser realitzada amb intervenció humana a causa de la gran quantitat de dades que han de ser processats) i queda alçada la prohibició, l'empresa haurà d'adoptar mesures adequades per salvaguardar els drets i llibertats i els interessos legítims de les persones treballadores (art. 22.3 RGPD).

Així i tot, en el supòsit en què pogués quedar alçada la prohibició, el Reglament General de Protecció de Dades estableix que les decisions automatitzades no podran basar-se en les categories especials de dades personals (p. ex., en dades de salut, dades que rellevin les opinions polítiques o l'afiliació sindical, etc.), excepte quan hi hagi hagut consentiment (art. 9.2.a)) o existeixi un interès públic essencial (art. 9.2.g)) (art. 22.4 RGPD). Tenint en consideració que el consentiment difícilment pot entendre's vàlid en les relacions en les quals hi hagi un contracte de treball i l'interès públic essencial generalment no serà aplicable en el compliment d'obligacions laborals, en principi, l'empresa no podrà utilitzar sistemes de control algorítmic que prenguin decisions automatitzades si empren dades personals especialment protegides.

> Les decisions automatitzades laborals no poden basar-se en dades personals especialment protegides.

4. Utilització de tècniques subliminars, manipuladores o enganyoses

El Reglament d'Intel·ligència Artificial (RIA) prohibeix la comercialització de sistemes d'IA que 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).

5. Reconeixement d'emocions

Igualment, es troba prohibit l'ús de sistemes d'IA que reconeguin emocions, és a dir, sistemes que emprin dades biomètriques, com, p. ex., el rostre o la veu, per distingir o inferir les emocions o les intencions de les persones; excepte quan el sistema sigui instal·lat per motius mèdics o de seguretat (art. 5.1.f) RIA). És important assenyalar que el Reglament d'Intel·ligència Artificial entén que 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. Queden igualment exclosos aquells sistemes que detectin expressions, gestos o moviments que resultin obvis, com un somriure, sempre que no s'emprin per deduir emocions. En definitiva, aquesta prohibició, dins dels sistemes de control algorítmic, implica que l'empresa no pot utilitzar la informació adquirida per detectar les emocions de les persones treballadores, ja que la seva instal·lació no respon a una finalitat mèdica o de seguretat.

6. Classificació d'informació sensible

Finalment, es prohibeix la comercialització de sistemes d'IA que emprin 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). Això significa que les empreses no poden utilitzar en el lloc de treball sistemes algorítmics de control que intentin "endevinar" aquestes característiques i classificar les persones treballadores d'acord amb elles.

A més de les prohibicions recollides en la normativa, el sistema de control algorítmic –en tenir un potencial impacte sobre els drets fonamentals de les persones treballadores– haurà de superar el principi de proporcionalitat. D'aquesta manera, abans d'implementar un sistema d'aquestes característiques, s'haurà d'acreditar:

a. que és idoni, és a dir, que és susceptible d'aconseguir l'objectiu proposat;

b. que és necessari, és a dir, que no existeix una altra mesura més moderada per a la consecució d'aquest objectiu i igual d'eficaç; i

c. que és proporcionat en sentit estricte, és a dir, que aporta més beneficis per a l'interès general que perjudicis sobre altres béns o valors en conflicte.

Així, aplicant el principi de proporcionalitat, l'empresa no podria instal·lar un sistema de control algorítmic si aquest pogués ser substituït per un altre sistema menys intrusiu i igual d'eficaç, i si els perjudicis que causa el sistema de control són desproporcionats en relació amb l'objectiu que es persegueix amb el seu ús i amb els beneficis que el mateix proporciona.

Ha d'informar l'empresa les persones treballadores quan s'instal·la un sistema de control algorítmic?

Si el mecanisme de control algorítmic incorpora sistemes de videovigilància, de geolocalització o implica l'ús d'un dispositiu digital propietat de l'empresa seran d'aplicació els deures d'informació disposats als articles 87, 89 i 90 de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD):

- Davant l'ús de dispositius de videovigilància, l'empresa haurà d'informar amb caràcter previ, i de manera expressa, clara i concisa, les persones treballadores sobre aquesta mesura (art. 89.1 LOPDGDD).
- Davant l'ús de sistemes de geolocalització, l'empresa, amb caràcter previ, haurà d'informar de manera expressa, clara i inequívoca a les persones treballadores sobre l'existència i característiques d'aquests dispositius, així com sobre el possible exercici dels drets d'accés, rectificació, limitació del tractament i supressió (art. 90.2 LOPDGDD).
- Davant l'ús de dispositius digitals propietat de l'empresa, les persones treballadores hauran de ser informades dels criteris d'utilització dels dispositius (art. 87.3 LOPDGDD); és a dir, de les prohibicions o autoritzacions d'ús, de la possibilitat de registre, de les eines de control que seran emprades per vigilar el compliment de les obligacions laborals, etc.

A més, quan el sistema de control algorítmic utilitzi dades personals de les persones treballadores, l'empresa haurà de respectar el dret d'informació establert en el Reglament General de Protecció de Dades (RGPD), 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 pel sistema de control algorítmic; 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 demostri la seva identitat per altres mitjans (art. 12.1 RGPD).

Finalment, el Reglament d'Intel·ligència Artificial també recull un deure d'informació. Per tant, quan el control algorítmic es realitzi a través 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).

Si es prenen decisions automatitzades, quins drets té la persona treballadora?

Les decisions individuals automatitzades, inclosa l'elaboració de perfils, que es nodreixen de dades personals, estan prohibides quan produeixen efectes jurídics en la persona objecte de la decisió o l'afecten significativament (art. 22.1 RGPD). No obstant això, aquesta prohibició s'alça en aquells supòsits en què la decisió és necessària per a la formalització o l'execució d'un contracte entre la persona interessada i la persona responsable del tractament (art. 22.2.a) RGPD), com podria ser-ho un contracte de treball, i s'acredita el caràcter necessari de la decisió automatitzada.

En aquests supòsits, quan les persones treballadores són objecte de decisions automatitzades, el Reglament General de Protecció de Dades preveu uns deures d'informació específics que han de ser complerts. L'empresa haurà de transmetre a les persones treballadores informació significativa sobre la lògica aplicada, així com la importància i les conseqüències previstes d'aquest tractament (arts. 13.2.f) i 14.2.g) RGPD). Aquests preceptes han estat interpretats en el sentit que la persona treballadora té dret a ser informada:

- Que està involucrada en un procés automatitzat de presa de decisions.
- Dels paràmetres que avalua l'algoritme i la ponderació d'aquests.
- De les conseqüències que tindrà la decisió automatitzada per a la persona treballadora.

A més, quan es prengui una decisió d'acord amb els resultats del sistema algorítmic i no hi hagi intervenció humana significativa, les persones treballadores tindran dret a obtenir intervenció humana, a expressar el seu punt de vista, a rebre una explicació de la decisió presa i a impugnar la decisió (art. 22.4 i Considerant 71 RGPD).

Si el sistema empra dades personals, quines obligacions ha de complir l'empresa?

Quan el sistema de control algorítmic utilitzi dades personals de les persones treballadores, l'empresa haurà de complir amb les garanties establertes en el Reglament General de Protecció de Dades:

- 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 "perfilat o valoració de subjectes, inclosa la recollida de dades del subjecte en múltiples àmbits de la seva vida (acompliment en el treball, personalitat i comportament)", "la presa de decisions automatitzades o que contribueixin en gran manera a la presa d'aquestes decisions" o "l'observació, monitoratge, supervisió, geolocalització o control de l'interessat de forma sistemàtica i exhaustiva".

  Per això, l'empresa haurà d'elaborar, amb caràcter previ a la instal·lació del sistema de control algorítmic, 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).

Pot un sistema de control algorítmic utilitzar dades relatives a la salut de la persona treballadora?

Hi ha sistemes de control algorítmic que analitzen la temperatura de la pell, la freqüència cardíaca, el flux sanguini o un altre tipus de dades relacionades amb la salut de les persones treballadores, a través de l'ús dels anomenats *wearable devices* (polseres o rellotges intel·ligents, jaquetes tecnològiques, etc.); i que permeten a l'empresa, en definitiva, monitorar la salut de les persones treballadores i obtenir informació per valorar l'aptitud de les matei-

xes en l'acompliment de l'activitat laboral. Per exemple, controlar les pulsacions pot indicar a l'empresa si una persona treballadora es troba en moviment i, per tant, si manté un ritme adequat de treball.

L'Agència Espanyola de Protecció de Dades, a la Guia sobre la protecció de dades en les relacions laborals va concloure que, aplicant el Reglament General de Protecció de Dades (RGPD), el monitoratge de dades de salut a través de dispositius intel·ligents es troba prohibit, amb caràcter general. Les dades de salut són dades considerades especialment sensibles pel RGPD. Això implica que sobre aquests recau una prohibició de tractament que exclusivament pot ser alçada quan concorre una de les circumstàncies o excepcions previstes a l'article 9.2 del RGPD. Dins d'aquestes excepcions s'inclou: que la persona presti el seu consentiment explícit, que el tractament sigui necessari per complir una obligació de Dret laboral o que el tractament sigui necessari per a fins de medicina preventiva o laboral. No obstant això, aquestes circumstàncies no són aplicables en el present supòsit perquè:

1. En l'àmbit de les relacions laborals, generalment, no serà considerat vàlid el consentiment en existir una desigualtat clara de poders.
2. No hi ha una norma de Dret laboral que reculli l'obligació de controlar la salut de les persones treballadores a través de dispositius intel·ligents.
3. El monitoratge de les dades de salut amb finalitats de control no s'emmarca en la vigilància de la salut per raons de prevenció de riscos laborals.

Amb tot això, l'Agència Espanyola de Protecció de Dades afegeix que el monitoratge permanent de les dades de salut en aquests supòsits vulnera el principi de proporcionalitat, en suposar l'accés a dades especialment sensibles sense respondre a una finalitat legítima.

Si el sistema de control algorítmic empra IA, quines obligacions ha de complir l'empresa?

El Reglament d'Intel·ligència Artificial (RIA) qualifica determinats sistemes com a sistemes d'IA d'alt risc. Aquesta qualificació –aplicable a aquells sistemes que puguin generar un major risc per als drets fonamentals– porta aparellada el compliment d'una sèrie de garanties reforçades. D'acord amb el

que estableix l'Annex III del RIA, són considerats sistemes d'IA d'alt risc aquells "destinats a ser utilitzats per prendre decisions que afectin les condicions de les relacions d'índole laboral o la promoció o rescissió de relacions contractuals d'índole laboral, per a l'assignació de tasques a partir de comportaments individuals o trets o característiques personals o per supervisar i avaluar el rendiment i el comportament de les persones en el marc d'aquestes relacions". Dins d'aquesta definició podrien quedar integrats, per tant, aquells sistemes de control algorítmic que utilitzen IA i que són utilitzats per a la presa de decisions relacionades amb el monitoratge, avaluació o supervisió de les persones treballadores.

En aquests supòsits, l'empresa, com a responsable del desplegament del sistema d'IA d'alt risc, haurà de garantir el compliment d'una sèrie obligacions, entre les quals es troben: adoptar mesures tècniques i organitzatives adequades per garantir que utilitzen aquests sistemes d'acord amb les instruccions d'ús que els acompanyin (art. 26.1 RIA); encomanar la supervisió humana del sistema a persones físiques que tinguin la competència, formació i autoritat necessàries (art. 26.2 RIA); vigilar el funcionament del sistema i suspendre l'ús i informar a l'entitat proveïdora o distribuïdora i l'autoritat competent quan seguir les instruccions pugui suposar un risc per a la salut, la seguretat o els drets fonamentals de les persones (art. 26.5 RIA); així com, complir amb els deures d'informació (art. 26.7 RIA).

A més, quan les persones treballadores es vegin afectades per l'ús de sistemes d'IA, 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.

Si el sistema de control algorítmic empra IA, quins drets addicionals tenen les persones treballadores?

El Reglament d'Intel·ligència Artificial reconeix un dret d'explicació (art. 86 RIA). En el supòsit en què l'empresa adopti decisions basades en els resultats d'un sistema d'IA d'alt risc (que produeixi efectes jurídics sobre la persona o l'afecti considerablement), la persona treballadora afectada tindrà dret a rebre una explicació clara i significativa sobre el paper que aquest sistema va desenvolupar en el procés de presa de decisions i sobre els principals elements que van conduir a la decisió adoptada.

L'ús de sistemes de control algorítmic pot suposar una vulneració de drets fonamentals?

L'ús de sistemes de control algorítmic permet a l'empresa exercir una vigilància molt més exhaustiva, constant i detallada sobre el rendiment i el comportament de les persones treballadores, la qual cosa pot traduir-se en una major ingerència en els seus drets fonamentals.

D'una banda, es poden veure lesionats el dret a la intimitat (art. 18.1 CE) i el dret a la protecció de dades (art. 18.4 CE), quan l'empresa instal·la un sistema de control algorítmic especialment invasiu, que no supera el principi de proporcionalitat o que incompleix la normativa vigent (p. ex., si s'ha incorporat una tecnologia de gravació de sons).

D'altra banda, l'ús de sistemes de control algorítmic també pot comprometre el dret fonamental a la no discriminació (art. 14 CE). Aquests sistemes solen alimentar-se de grans volums de dades que, a vegades, poden estar esbiaixats o poden realitzar correlacions estadístiques que deriven en la perpetuació de resultats discriminatoris. A més, cal ressaltar que fins i tot quan no s'empren directament dades vinculades a categories protegides (com el sexe, l'edat, l'orientació sexual o l'afiliació sindical), els algoritmes poden inferir aquestes característiques a partir d'altres variables aparentment neutres (per exemple, el codi postal, hàbits de navegació o patrons de conducta), la qual cosa pot ocasionar de nou la perpetuació de pràctiques discriminatòries.

Aquestes dinàmiques poden donar lloc tant a discriminació directa (quan l'algoritme es basa en una categoria protegida per decidir (p. ex., en l'origen ètnic, la condició social o l'orientació sexual de les persones treballadores)), com a discriminació indirecta (quan a partir de dades aparentment neutres es produeix un impacte advers injustificat sobre un grup protegit). La manca de transparència inherent a molts sistemes automatitzats dificulta, a més, la identificació i prova d'aquestes discriminacions. Per fer front a aquest risc, han sigut incorporades salvaguardes específiques en la normativa. Per exemple, la Llei integral per a la igualtat de tracte i la no discriminació, estableix que les administracions públiques i les empreses promouran l'ús d'una Intel·ligència Artificial ètica, confiable i respectuosa amb els drets fonamentals (art. 23.3).

En tot cas, davant una potencial lesió de drets fonamentals per part de l'empresa, 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 (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.

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

Si l'empresa infringeix la normativa laboral aplicable a l'ús de sistemes de control algorítmic en el lloc de treball, les persones treballadores i/o la representació legal poden denunciar aquesta situació davant la Inspecció de Treball i Seguretat Social.

Entre les infraccions que podrien ser sancionades per la ITSS es troben:

- Infraccions molt greus que poden ser sancionades 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 (art. 40.1.1.c) LLISOS):
  - Els actes de l'empresa que siguen contraris al respecte a la intimitat i consideració deguda a la dignitat de les persones treballadores (art. 8.11 LISOS).
  - Les decisions unilaterals de l'empresa que impliquin discriminacions directes o indirectes desfavorables per raó d'edat o discapacitat o favorables o adverses en matèria de retribucions, jornades, formació, promoció i altres condicions de treball, per circumstàncies de sexe, origen, inclòs el racial o ètnic, estat civil, condició social, religió o conviccions, idees polítiques, orientació i identitat sexual, expressió de gènere, característiques sexuals, adhesió o no a sindicats i als seus acords, vincles de parentiu amb altres persones treballadores a l'empresa o llengua dins de l'Estat espanyol [...] (art. 8.12 LLISOS).

Pot ser sancionada l'empresa per un 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'actuació[1]). 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).

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

  - La falta d'adopció de mesures les 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.

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

- 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, les persones treballadores podran presentar reclamació davant l'Agència Espanyola de Protecció de Dades o davant l'Autoritat Catalana de Protecció de Dades per falta d'atenció d'una sol·licitud d'exercici dels drets d'accés, rectificació, limitació del tractament i supressió.

Quines implicacions pot tenir l'ús de sistemes de control algorítmic sobre la salut de les persones treballadores?

La introducció de sistemes de control algorítmic en el lloc de treball pot tenir efectes negatius en la salut de les persones treballadores. El constant monitoratge i observació de la persona treballadora és un factor de risc psicosocial que pot propiciar l'aparició de patologies com estrès, ansietat o depressió[2]. Un exemple d'aquesta situació és l'impacte dels sistemes reputacionals basats en avaluacions de clients, que poden generar una pressió addicional en obligar la persona a mostrar-se constantment amable o somrient per evitar valoracions –i conseqüències– negatives, fet que incrementa la càrrega emocional i el risc d'estrès. Igualment, quan s'empren sistemes de control algorítmic que, per exemple, marquen el ritme i la càrrega de treball, també es posa en risc la salut física de les persones treballadores, en exercir una pressió sobre la persona que incrementa el risc d'accidents de treball –i de nou de riscos psicosocials–.

De fet, el Tribunal Superior de Justícia del País Basc en la seva Sentència núm. 1431/2016, de 5 de juliol de 2016 va considerar que l'excessiu control, desconfiança i pressió cap a una persona treballadora eren indicis que indicaven que l'entorn laboral no proporcionava un clima de seguretat i salut adequat.

De forma més concreta, la Sentència del Tribunal Superior de Justícia de Catalunya núm. 3613/2013, de 23 de maig de 2013 va entendre que l'ús d'un acceleròmetre i sistema GPS als telèfons mòbils atorgats a les persones treballadores per detectar el moviment i l'absència del mateix suposava un agressiu aparell de control que podia posar en risc la salut de les persones treballadores. En aquest supòsit, a més, les persones treballadores eren responsables del dispositiu fora de l'horari de treball, havent de garantir que es trobés en condicions òptimes per al seu bon funcionament durant la jornada laboral. El Tribunal Superior de Justícia de Catalunya va considerar que l'estrès, la tensió i la preocupació que comportava aquesta responsabilitat eren riscos psicosocials que l'empresa havia d'haver previst.

2 Criteri Tècnic 104/2021, sobre actuacions de la Inspecció de Treball i Seguretat Social en riscos psicosocials i en la Nota Tècnica Preventiva 1.113: Les Tecnologies de la Informació i la Comunicació (TIC) (II): factors de risc psicosocial.

Els sistemes de control algorítmic poden generar riscos psicosocials i físics en el lloc de treball, ja que el monitoratge constant, la pressió i la gestió automatitzada de la càrrega i el ritme de treball poden provocar estrès, ansietat i fins i tot accidents laborals. Per això, l'empresa té el deure d'avaluar aquests riscos, aplicar mesures preventives, formar el personal i informar-lo adequadament, així com consultar la representació de les persones treballadores sobre la seva implantació.

En tot cas, davant els canvis tecnològics que puguin produir-se en el lloc de treball, l'empresa té el deure de garantir la seguretat i la salut de les persones treballadores (art. 14.2 LPRL). Aquest deure es concreta en:

- L'obligació d'avaluar els riscos laborals (art. 16.2.a) LPRL), en aquest cas, lligats a l'ús dels sistemes de videovigilància.
- L'obligació d'implementar mesures preventives per eliminar o reduir i controlar els riscos manifestats (art. 16.2.b) LPRL).
- L'obligació de garantir que cada persona treballadora rebi una formació teòrica i pràctica suficient i adequada en matèria preventiva quan s'introdueixin noves tecnologies (art. 19.1 LPRL), com podria ser-ho un sistema de videovigilància.

A més, l'empresa haurà de consultar a les persones delegades de prevenció la introducció dels sistemes de control algorítmic en relació amb el seu possible impacte en la seguretat i salut de les persones treballadores (art. 33.1.a) LPRL), i debatre amb el Comitè de Seguretat i Salut la introducció de noves tecnologies pel que fa a la seva incidència en la prevenció de riscos (art. 39.1.a) LPRL). En tot cas, aquests deures de consulta es complementen amb el deure d'informar les persones treballadores sobre els riscos que plantegen els sistemes de control algorítmic per a la seva seguretat i salut i les mesures de prevenció aplicables (art. 18.1 LPRL), reconeixent la normativa a les persones treballadores el dret a efectuar propostes (art. 18.2 LPRL).

Quines conseqüències té l'incompliment de la normativa en matèria de prevenció de riscos laborals?

L'incompliment de la normativa en matèria de prevenció de riscos laborals 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).

  - 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).

Drets col·lectius davant el control tecnològic

Té dret la RLPT a ser informada i consultada sobre la instal·lació de sistemes de control en el lloc de treball (sistemes de videovigilància, geolocalització, etc.)?

La RLPT té dret a ser informada i consultada per l'empresa sobre aquelles qüestions que puguin afectar les persones treballadores (art. 64.1 ET), la qual cosa inclou la instal·lació de sistemes destinats a vigilar el compliment de les obligacions laborals (p. ex., sistemes de videovigilància, de geolocalització, algorítmics, etc.). La implementació d'aquest tipus de tecnologies en l'àmbit laboral implica la implantació de sistemes d'organització i control del treball, per la qual cosa, en aplicació de l'art. 64.5.f) ET, la representació legal tindrà dret a emetre un informe, amb caràcter previ a l'execució de la decisió empresarial.

L'incompliment del dret d'informació i consulta pot suposar la nul·litat de la mesura empresarial i una vulneració de drets fonamentals (dret a la llibertat sindical) quan no es permet la participació de la representació sindical. A més, la Inspecció de Treball i Seguretat Social podria aplicar una sanció per la transgressió dels drets d'informació, audiència i consulta de la representació de les persones treballadores (arts. 7.7 i 40.1.b) LISOS).

Així mateix, la normativa espanyola sobre protecció de dades, és a dir, la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals també reconeix drets d'informació específics en relació amb la implementació de sistemes de videovigilància i geolocalització:

- Amb caràcter previ a la instal·lació d'un sistema de videovigilància, l'empresa haurà d'informar de manera expressa, clara i concisa a la RLPT sobre aquesta mesura (art. 89.1 LOPDGDD).
- Amb caràcter previ a la instal·lació d'un sistema de geolocalització, l'empresa haurà d'informar de manera expressa, clara i inequívoca a la RLPT sobre l'existència i característiques d'aquests dispositius (art. 90.2 LOPDGDD).

Té dret la RLPT a ser informada sobre la implementació d'un sistema algorítmic o d'IA en el lloc de treball?

La representació legal de les persones treballadores té reconegut el dret d'informació algorítmica (art. 64.4.d) ET). Quan l'empresa empra "algoritmes o sistemes d'intel·ligència artificial que afecten la presa de decisions que puguin incidir en les condicions de treball, l'accés i manteniment de l'ocupació, inclosa l'elaboració de perfils", la RLPT té dret a ser informada, amb la periodicitat que procedeixi, "dels paràmetres, regles i instruccions" en els quals es basen aquests sistemes.

En relació amb aquest dret d'informació, el 2022, el Ministeri de Treball i Economia Social va publicar la "Guia pràctica i eina sobre l'obligació empresarial d'informació sobre l'ús d'algoritmes en l'àmbit laboral". S'hi va plasmar que l'obligació d'informació sobre "els paràmetres, regles i instruccions" s'havia d'interpretar com una obligació de l'empresa de comunicar informació relativa a: "(a) les variables i els paràmetres, entesos com la importància relativa de cada variable en l'algoritme; i (b) les regles i instruccions, referents a les regles de programació que condueixen a la presa de la decisió". Aquesta informació haurà de ser facilitada a la RLPT amb la periodicitat que procedeixi i, en tot cas, prèvia utilització dels sistemes algorítmics o d'IA i davant qualsevol canvi en les característiques del sistema. A més, a banda del dret d'informació algorítmica, quan s'empren sistemes d'IA d'alt risc en el lloc de treball s'aplica el dret d'informació recollit a l'article 26.7 del Reglament d'Intel·ligència Artificial. Aquest precepte imposa a l'empresa l'obligació d'informar els òrgans de representació de les persones treballadores afectades que estaran exposades a la utilització d'un sistema d'IA d'alt risc, en tot cas abans del seu ús.

Dins dels sistemes d'IA d'alt risc, queden inclosos aquells que són destinats a ser utilitzats per a "la contractació o la selecció de persones físiques, en particular per a publicar anuncis d'ocupació específics, analitzar i filtrar les sol·licituds d'ocupació i avaluar als candidats"; o per "prendre decisions que afectin les condicions de les relacions d'índole laboral o la promoció o rescissió de relacions contractuals d'índole laboral, per a l'assignació de tasques a partir de comportaments individuals o trets o característiques personals o per supervisar i avaluar el rendiment i el comportament de les persones en el marc d'aquestes relacions" (Annex III, l'apartat 4 RIA).

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.

Té dret la RLPT a ser informada i consultada sobre la implementació de tecnologies quan aquestes poguessin tenir un impacte sobre la seguretat i salut de les persones treballadores?

La introducció de mitjans tecnològics en el lloc de treball, com sistemes de videovigilància, geolocalització o control algorítmic pot tenir una repercussió negativa sobre la seguretat i salut de les persones treballadores (creant nous perills o potenciant riscos físics o psicosocials ja existents). Per això, les persones delegades de prevenció hauran de ser consultades 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). A més, el Comitè de Seguretat i Salut podrà participar en l'elaboració i avaluació dels plans i programes de prevenció de riscos de l'empresa i debatre, a aquest efecte, la introducció de noves tecnologies (art. 39.1.a) LPRL).

En tot cas, els òrgans de representació tenen dret a ser consultats sobre qualsevol acció que pugui tenir efectes substancials sobre la seguretat i salut de les persones treballadores (art. 33.1.f) 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 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 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).

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).

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 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

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 del control continu i individualitzat

El conveni pot prohibir l'ús de sensors o sistemes algorítmics o d'IA que permetin un seguiment constant i individualitzat de la persona treballadora. Com es recull en l'apartat 2.6 de la guia, el control permanent és un factor de risc psicosocial que pot generar estrès, pressió i afectar la salut mental.

Així, si escau, només s'haurien de permetre mesures puntuals i estrictament necessàries.

Limitació estricta del tipus de dades recollides

Els sistemes algorítmics o d'IA que són emprats en l'empresa, en ocasions, recopilen informació personal de les persones treballadores. Com ha estat assenyalat en l'apartat 2.6 de la guia, hi ha sistemes que per ser especialment invasius es troben prohibits amb caràcter general per la normativa: sistemes que recopilen dades biomètriques o de salut, sistemes que reconeixen emocions, etc.

Per a reforçar aquesta protecció que atorga la llei, el conveni pot establir expressament que els sistemes només puguin recollir dades estrictament necessàries per a la salud de la persona treballadora. A més de nou, es molt important que se pacte que qualsevol ús d'aquestes dades per a finalitats diferents de la prevenció, i especialment per a finalitats disciplinaries, es consideraria una vulneració del dret a la intimitat de la persona treballadora.

Limitació temporal i supressió de dades

El conveni pot establir que les dades recollides s'eliminin en el menor temps possible.Només es poden conservar mentre siguin necessàries per a la finalitat preventiva. Un cop desaparegui el risc, les dades s'han de suprimir automàticament.

Prohibició de decisions automatitzades

El conveni hauria de prohibir que les dades obtingudes per sensors o sistemes d'IA s'utilitzin per prendre decisions basades exclusivament en processos automatitzats. No es poden adoptar sancions, canvis de lloc de treball o valoracions negatives sense intervenció humana. La falta de transparència en les decisions automatitzades dificulta que les persones treballadores puguin obtenir una explicació del perquè de la decisió i que puguin, al cap i a la fi,

qüestionar-la. Per aquesta raó, les persones treballadores han de tenir sempre una persona responsable identificable de les decisions preses.

A més, el conveni hauria de reconèixer el dret de les persones treballadores a revisar les decisions que han estat adoptades per l'empresa amb suport d'un sistema automatitzat i a obtenir una explicació sobre el paper que el sistema ha tingut en la presa de la decisió.

Prohibició de discriminació

El conveni hauria de reconèixer el dret a la no discriminació en l'ús de sistemes algorítmics o d'IA i en la presa de decisions automatitzades. L'empresa ha de garantir que els sistemes algorítmics o d'IA no generin biaixos discriminatoris.

Per a garantir una protecció reforçada i supervisar que els sistemes algorítmics o d'IA no perpetuïn pràctiques discriminatòries, el conveni pot preveure la **realització periòdica d'auditories externes** a càrrec de l'empresa i previ acord amb la representació legal dels seus termes.

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 representació 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'us de qualsevols 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'us de qualsevols sistema de control per part de l'empresa que no sigui 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'us de eines de control tecnològic.

Sense aquesta avaluació, no s'hauria de permetre la seva utilització i pactar expressament que l'us 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.


UGT.cat

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

Control algorítmic

4

UGT.cat