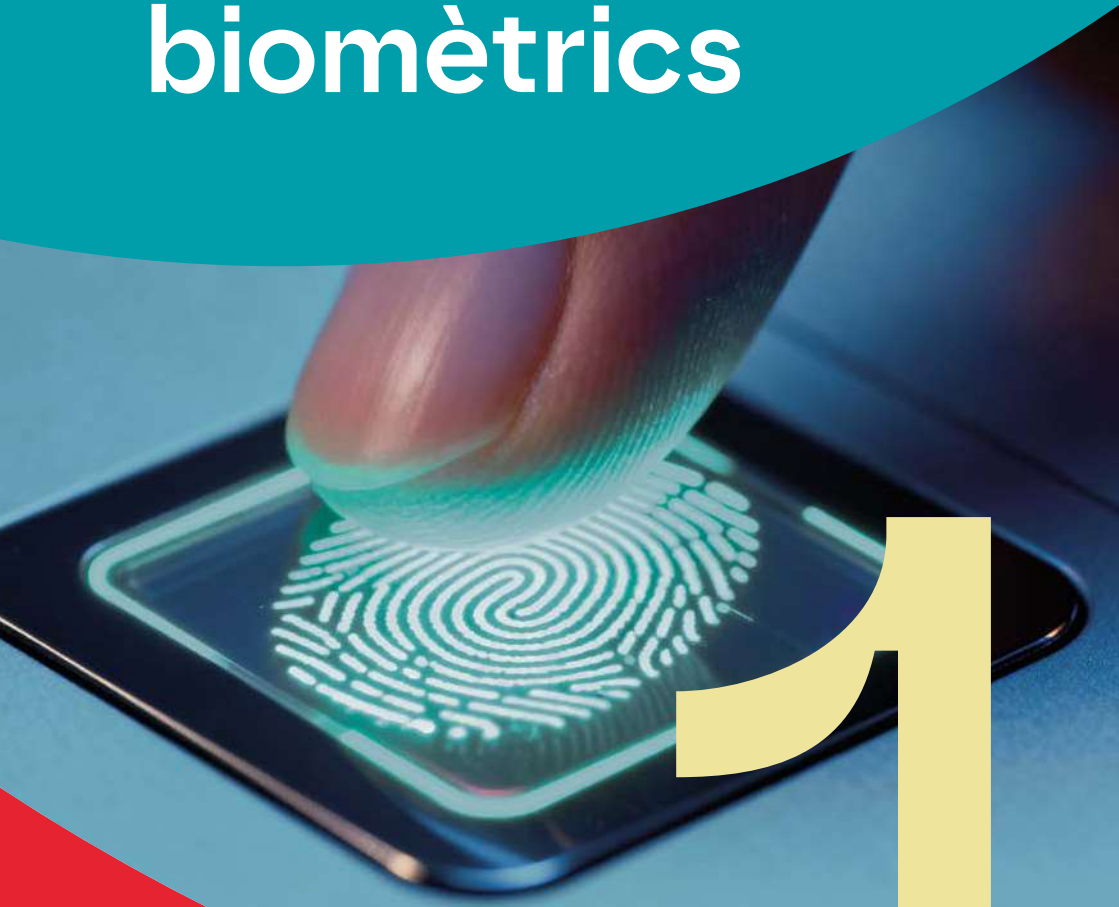
Guia de drets laborals i de prevenció de riscos: IA i vigilància tecnològica

Sistemes biomètrics



1

UGT.cat

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

Sistemes biomètrics

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 11741-2026

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

Sistemes biomètrics

1

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 l'ús de sistemes biomètrics

Què són les dades biomètriques i per què es consideren especialment sensibles?

D'acord amb el Reglament General de Protecció de Dades (RGPD), les dades biomètriques són dades personals obtingudes a partir d'un tractament tècnic específic, relatives a les característiques físiques, fisiològiques o conductuals d'una persona física que permeten o confirmen la identificació única d'aquesta persona (art. 4.14 RGPD). Dins d'aquesta tipologia de dades queden inclosos múltiples trets de les persones treballadores tals com: el rostre, l'empremta dactilar, l'iris, la retina, la veu, l'ADN, la forma de caminar o moure's, etc.

En definitiva, són dades que es troben estretament vinculades a una persona i que permeten distingir-la. Atès que es tracta d'informació de la qual la persona no pot desprendre's amb caràcter general, la seva utilització pot tenir un impacte més elevat en els drets i llibertats fonamentals de la persona titular d'aquestes. A més, el tractament d'aquestes dades personals pot facilitar a l'empresa l'accés a informació sensible relacionada amb la salut de les persones treballadores, el seu origen ètnic i fins i tot les seves opinions i conviccions polítiques.

Per aquestes raons, el Reglament General de Protecció de Dades ha reconegut les dades biomètriques dirigides a identificar de manera unívoca una persona física una protecció reforçada, considerant-les especialment sensibles i incloent-les dins de les categories especials de dades personals (art. 9.1 RGPD).

Què implica que les dades biomètriques pertanyin a les categories especials de dades personals?

El Reglament General de Protecció de Dades (RGPD) qualifica les dades biomètriques com a dades especialment sensibles, és a dir, com a dades que requereixen d'una major protecció; i per això prohibeix el seu tractament amb caràcter general. Això implica que només podran ser tractades les dades biomètriques de les persones treballadores –dirigides a identificar-les– quan concorri una de les condicions –o excepcions a la prohibició– recollides a l'article 9.2 del RGPD. En el context laboral, podrien ser aplicables tres excepcions principalment:

a. Que la persona treballadora presti el seu consentiment (art. 9.2.a) RGPD). Ha de ser assenyalat que, generalment, en l'àmbit de les relacions laborals, no serà considerat vàlid el consentiment en existir una desigualtat clara de poders.

b. Que el tractament sigui necessari per complir obligacions i per exercir els drets específics de la persona responsable del tractament (l'empresa) o de la persona interessada (la persona treballadora), en l'àmbit del dret laboral i de la seguretat i la protecció social, si ho autoritza el dret de la Unió o dels estats membres o un conveni col·lectiu (art. 9.2.b) RGPD).

c. Que el tractament sigui necessari per a finalitats de medicina preventiva o laboral, d'avaluació de la capacitat laboral de la persona treballadora, de diagnòstic mèdic, de prestació d'assistència o de tractament de tipus sanitari o social, o de gestió dels sistemes i serveis d'assistència sanitària i social (art. 9.2.h) RGPD).

Fora d'aquests supòsits, l'empresa, en principi, no podria emprar les dades biomètriques per distingir una persona treballadora.

Quins principis ha de complir l'empresa en emprar sistemes biomètrics?

Qualsevol tractament de dades personals ha de complir els principis relatius al tractament recollits en el Reglament General de Protecció de Dades (art. 5 RGPD): el principi de licitud, lleialtat i transparència; el principi de limitació de la finalitat; el principi de minimització de dades; el principi d'exactitud; el principi de limitació del termini de conservació; el principi d'integritat i confidencialitat; el principi d'integritat i confidencialitat; i el principi de responsabilitat proactiva.

Dins d'aquests principis, cal destacar el principi de minimització de dades que exigeix que les dades emprades siguin adequades, pertinents i limitades al que és necessari en relació amb les finalitats per a les quals són tractades (art. 5.1.c) RGPD). Aquest principi suposa que únicament hauran de ser utilitzades les dades biomètriques de les persones treballadores quan la finalitat del tractament d'aquesta dada personal no pugui aconseguir-se raonablement per altres mitjans. D'altra banda, l'article 5 del RGPD també recull el principi de limitació de la finalitat, el qual preveu que les dades no podran ser tractades posteriorment de manera incompatible amb els fins expressos per als quals van ser recollides (art. 5.1.b) RGPD).

A més, el sistema de biometria que implementi l'empresa 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.

Aplicant el principi de proporcionalitat s'haurà d'avaluar, per tant, si existeix un altre sistema menys intrusiu i igual d'eficaç –que un sistema de biometria, en aquest cas– que pugui complir amb la finalitat prevista, i si els perjudicis causats pel sistema que es pretén implementar no són desproporcionats en relació amb l'objectiu perseguit.

Quines obligacions té l'empresa en implantar sistemes que tracten dades biomètriques?

Les dades biomètriques són considerades dades especialment sensibles, per la qual cosa, amb caràcter general, el seu tractament es troba prohibit (art. 9.1 RGPD). Aquesta prohibició pot ser alçada quan confluеix una de les excepcions establertes a l'article 9.2 del Reglament General de Protecció de Dades (RGPD). Per això, en primer lloc, l'empresa haurà de cerciorar-se que el seu tractament es troba justificat en base a una d'aquestes excepcions.

En segon lloc, si s'alça la prohibició de tractament, l'empresa haurà d'acreditar que el tractament és lícit, és a dir, que concorre una de les condicions legitimadores del tractament recollides a l'article 6 del RGPD. Amb caràcter general, s'aplicarà l'establerta en la lletra b): «el tractament és necessari per executar un contracte en el qual l'interessat és part [...]».

En tercer lloc, l'empresa haurà d'elaborar una **avaluació d'impacte relativa a la protecció de dades**. Quan el tractament de dades personals pugui implicar un alt risc per als drets i llibertats de les persones, l'article 35 del RGPD exigeix la realització d'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[1] aquells «que impliquin l'ús de categories especials de dades a què es refereix l'article 9.1 del RGPD» i aquells «que impliquin l'ús de dades biomètriques amb el propòsit d'identificar de manera única una persona física». En conseqüència, quan l'empresa tracti dades biomètriques haurà de dur a terme l'avaluació d'impacte relativa a la protecció de dades amb caràcter previ a l'inici del tractament, i aquesta haurà d'incloure, almenys:

a. Una descripció sistemàtica de les operacions de tractament previstes i de les finalitats del tractament, inclòs, si escau, l'interès legítim perseguit per la persona responsable del tractament.

b. Una avaluació de la necessitat i la proporcionalitat de les operacions de tractament respecte amb la seva finalitat.

c. Una avaluació dels riscos per als drets i llibertats de les persones.

d. Les mesures previstes per afrontar els riscos, incloses garanties, mesures de seguretat i mecanismes que garanteixin la protecció de dades personals, i per demostrar la conformitat amb aquest Reglament, tenint en compte els drets i interessos legítims de les persones interessades i d'altres persones afectades.

En relació amb la implementació de mesures de seguretat adequades, l'Agència Espanyola de Protecció de Dades recull, a la Guia sobre la protecció de dades en les relacions laborals, una sèrie de garanties que l'empresa hauria de complir:

- **Emmagatzematge com a plantilles biomètriques**. Les dades biomètriques hauran de ser emmagatzemades com a plantilles biomètriques, sempre que sigui possible. Les plantilles biomètriques no guarden la imatge de la dada biomètrica original, sinó un patró o punts distintius de la dada biomètrica.

- **Emmagatzematge personal**. Les dades biomètriques s'han de guardar preferiblement en un dispositiu personal de la persona treballadora (com pot ser una targeta), no en un sistema central. A més, s'ha de fer servir una clau d'encriptat especial per protegir-los d'accessos no autoritzats.

- **Ús exclusiu.** El sistema biomètric i les seves mesures de seguretat han d'assegurar que les dades no es puguin fer servir per a altres finalitats diferents a les inicialment previstes.

1 Vegeu: www.aepd.es/documento/listas-dpia-es-35-4.pdf

- **Protecció amb xifrat.** S'han de fer servir tecnologies de xifrat per evitar que les dades siguin llegides, copiades, modificades o eliminades sense autorització.
- **Possibilitat de revocar la identitat.** Els sistemes han de permetre que, si cal, es pugui anul·lar el vincle entre la persona i les seves dades biomètriques.
- **Evitar interconnexions entre bases de dades.** S'han de fer servir formats o tecnologies que impedeixin unir diferents bases de dades biomètriques.
- **Eliminació de dades.** Les dades biomètriques s'han de suprimir quan ja no siguin necessàries per al propòsit amb què es van recollir. Si es pot, s'ha d'introduir la supressió automatitzada.

S'ha d'informar les persones treballadores sobre la instal·lació de sistemes de biometria?

L'empresa haurà d'informar les persones treballadores sobre les finalitats per a les quals es fan servir les dades biomètriques; les persones destinatàries de la informació; el termini durant el qual es conservaran les dades biomètriques; la possibilitat d'exercir els drets d'accés, rectificació, supressió, limitació del tractament i portabilitat de les dades; 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).

Els drets de les persones treballadores en matèria de protecció de dades estan compostos per:

- **El dret d'accés a les dades personals** (art. 15 RGPD). La persona treballadora podrà demanar a l'empresa que li confirmi si estan sent tractades les seves dades biomètriques i, en tal cas, que li proporcioni informació sobre les característiques del tractament.
- **El dret de rectificació de les dades personals** (art. 16 RGPD). La persona treballadora té dret a demanar a l'empresa que rectifiqui o completi dades personals que sigui inexactes o estiguin incompletes.
- **El dret de supressió de les dades personals** (art. 17 RGPD). La persona treballadora té dret a demanar la supressió de les dades biomètriques. L'empresa estarà obligada a suprimir-los sense dilació indeguda si ja no són necessaris o han estat obtinguts il·lícitament, és a dir, incomplint la

normativa. No obstant això, és important tenir en compte que les dades no podran ser eliminades si la seva conservació és necessària per al compliment d'una obligació legal.

- **El dret a la limitació del tractament de les dades personals** (art. 18 RGPD). La persona treballadora pot demanar que les seves dades biomètriques no siguin utilitzades temporalment per a certes finalitats. L'exercici d'aquest dret implica que l'empresa podrà emmagatzemar les dades, però no utilitzar-les, excepte en situacions excepcionals, p. ex., per a l'exercici o defensa de reclamacions, la protecció dels drets d'una altra persona o per raons d'interès públic.
  Aquest dret es pot invocar quan:
  - S'impugna l'exactitud de les dades personals.
  - El tractament de les dades és il·lícit.
  - L'empresa ja no necessita les dades, però la persona treballadora les requereix per defensar alguna reclamació.
  - La persona treballadora s'ha oposat al tractament i està pendent de resoldre's l'oposició.
- **El dret a la portabilitat de les dades** (art. 20 RGPD). La persona treballadora tindrà dret a rebre les dades biomètriques que ha facilitat i a transmetre'ls a una altra persona responsable del tractament.

Quina diferència hi ha entre autenticació i identificació?

Quan les dades biomètriques són tractades per distingir una persona treballadora, aquestes poden ser utilitzades emprant processos de:

- **Autenticació**. L'autenticació té lloc quan es verifica i confirma que una persona és qui afirma ser. Es tracta d'un procés en el qual es comparen les dades biomètriques de la persona únicament amb les dades recollides prèviament en una plantilla o mostra biomètrica vinculada a la seva identitat. La comparació és un-a-un (1:1).
- **Identificació**. La identificació té lloc quan es busca localitzar una persona dins d'un grup d'individus. Es tracta d'un procés en el qual es comparen les dades biomètriques de la persona treballadora amb les dades d'un conjunt ampli de persones recollides en una base de dades. D'aquesta manera, s'evidencia si la dada introduïda coincideix amb alguna de les dades emmagatzemades en el sistema. La comparació és un-a-diversos (1:N).

Independentment que el tractament de dades biomètriques s'efectuï a través d'un procés d'autenticació o d'identificació, s'entendrà que s'està duent a terme un tractament de categories especials de dades conforme a l'article 9 del Reglament General de Protecció de Dades. Aquest criteri va ser recollit pel Comitè Europeu de Protecció de Dades en les Directrius 5/2022 sobre l'ús de la tecnologia de reconeixement facial en l'àmbit de l'aplicació de la llei[2].

Tanmateix, és rellevant remarcar que els riscos que planteja l'autenticació i la identificació difereixen. L'Agència Espanyola de Protecció de Dades, en la resolució a la consulta prèvia amb referència REGAGE25e00024730156[3], recorda que els processos d'identificació poden tenir un major impacte sobre els drets i llibertats fonamentals, principalment pel seu caràcter invasiu i pel seu potencial abast a un nombre més elevat de persones; mentre que l'autenticació resulta generalment ser menys intrusiva. En conseqüència, l'Agència Espanyola de Protecció de Dades considera que les garanties que exigeix la normativa (demostrar la necessitat i proporcionalitat, aixecar la prohibició de tractament, etc.) han de ser valorades amb diferent intensitat depenent del tipus de tecnologia que es tracti, exigint a la identificació una motivació més rigorosa.

Quins són els principals usos que poden tenir els sistemes biomètrics en l'àmbit laboral?

Les principals funcions que han estat reconegudes als sistemes biomètrics en l'àmbit laboral són: el registre de jornada i control de presència, el control d'accés a instal·lacions o dispositius amb finalitats no laborals, l'exercici de les facultats de control i la supervisió de l'activitat laboral i la vigilància de la salut i prevenció de riscos laborals. A més, les tecnologies de biometria es poden combinar amb sistemes d'intel·ligència artificial per complir objectius addicionals, com esdevé, per exemple, amb els sistemes de reconeixement d'emocions.

No obstant això, la possibilitat de tractar dades biomètriques amb aquestes finalitats no suposa que sigui legítim i lícit el seu tractament en tot cas. S'haurà d'atendre, en primer lloc, les obligacions que neixen de la normativa vigent.

> Els sistemes biomètrics permeten controlar accessos, jornada i activitat laboral sota límits legals estrictes.

2 Vegeu: www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_es.pdf

3 Vegeu: www.aepd.es/documento/regage25e00024730156.pdf

Registre de jornada i control d'accés o presència amb fins laborals

Es poden emprar tecnologies de biometria per registrar la jornada de treball o controlar la presència de les persones treballadores?

L'empresa té l'obligació de registrar la jornada diària de cada persona treballadora, incloent-hi l'horari concret d'inici i finalització de la jornada de treball (art. 34.9 ET). La normativa no estableix una forma concreta en la qual s'hagi d'efectuar el registre de jornada, havent reconegut el Ministeri de Treball, Migracions i Seguretat Social, a la Guia sobre el registre de jornada, que s'admet «qualsevol sistema o mitjà, en suport paper o telemàtic, apte per complir l'objectiu legal, això és, proporcionar informació fiable, immodificable i no manipulable a posteriori». En tot cas, el sistema haurà de proporcionar informació objectiva, fiable i accessible (Sentència del Tribunal de Justícia de la Unió Europea, de 14 de maig de 2019 (assumpte C-55/18)).

Sota aquestes premisses, es podria entendre que és vàlid l'ús de tecnologies de biometria (p. ex., sistemes de reconeixement facial o d'escàner d'empremta dactilar) per garantir el compliment de l'obligació de registre horari. No obstant això, com s'està duent a terme un tractament de dades biomètriques, en tot cas, s'ha de complir amb la normativa en matèria de protecció de dades.

El Reglament General de Protecció de Dades (RGPD) qualifica les dades biomètriques com a dades especialment sensibles, per la qual cosa el seu tractament es troba prohibit tret que es compleixi alguna de les excepcions previstes en la norma (art. 9.2 RGPD). En el present supòsit, a banda de la possibilitat que les persones treballadores prestessin el seu consentiment (una opció que en escassos supòsits s'entén vàlida), podria ser d'aplicació l'excepció prevista en la lletra b): «el tractament és necessari per complir obligacions i per exercir els drets específics del responsable del tractament o de l'interessat, en l'àmbit del dret laboral i de la seguretat i la protecció social, si ho autoritza el dret de la Unió o dels estats membres o un conveni col·lectiu conforme al dret dels estats membres que estableixi garanties adequades del respecte dels drets fonamentals i dels interessos de l'interessat». Aquesta excepció és aplicable quan existeix una obligació recollida en el Dret laboral que autoritzi el tractament de les dades biomètriques.

L'Agència Espanyola de Protecció de Dades, a la Guia sobre tractaments de control de presència mitjançant sistemes biomètrics[4], sosté que l'obligació legal de registre horari de l'article 34.9 ET no conté «cap autorització prou específica per considerar necessari el tractament de dades biomètriques amb la finalitat d'un control horari de la jornada de treball». La normativa no solament hauria de fer menció expressa a la possibilitat d'emprar tecnologies de biometria, sinó que en estar afectant un dret fonamental hauria de preveure i regular garanties que asseguressin la seva protecció (Sentència del Tribunal Constitucional núm. 76/2019, de 22 de maig). L'exigència d'establir garanties també és recollida en el mateix article 9.2.b) del RGPD.

En absència d'aquests elements, l'Agència Espanyola de Protecció de Dades entén que no queda alçada la prohibició de tractament que recau sobre aquesta categoria especial de dades personals. Per això, en principi, des de la perspectiva de protecció de dades, no podrien ser tractades les dades biomètriques amb finalitats de registre horari.

A més, encara que s'establís expressament en la normativa que les dades biomètriques poden ser emprades per al compliment de l'obligació de registre, l'empresa hauria d'acreditar que el sistema biomètric és necessari (art. 9.2.b) RGPD). Segons estableix l'Agència Espanyola de Protecció de Dades, a la Guia sobre tractaments de control de presència mitjançant sistemes biomètrics, el caràcter necessari del tractament implica que l'empresa haurà de justificar les circumstàncies per les quals ja no és possible utilitzar els sistemes de registre que s'han fet servir fins al moment i les raons per les quals ja no són adequats aquests sistemes.

Amb tot això, cal puntualitzar que abans de l'aprovació del Reglament General de Protecció de Dades, la jurisprudència sí que admetia, amb caràcter general, l'ús de dades biomètriques amb finalitats de control horari, en considerar-les un mitjà proporcionat per al compliment d'aquesta obligació (Sentència del Tribunal Suprem, Sala Contenciosa Administrativa, de 2 de juliol de 2007 (rec. 5017/2003); Sentència del Tribunal Superior de Justícia de Cantàbria, Sala Contenciosa Administrativa, de 10 de gener de 2003 (rec. 517/2002); Sentència del Tribunal Superior de Justícia de la Regió de Múrcia, Sala Social, núm. 47/2010, de 25 de gener de 2010).

Pel que fa al tractament de dades biomètriques per controlar la presència de les persones treballadores, serien d'aplicació els mateixos criteris; entenent, de nou, que no existeix una obligació prou expressa que permeti alçar la prohibició de tractament.

4 Vegeu: www.aepd.es/guias/guia-control-presencia-biometrico.pdf

Control d'accés amb finalitats no laborals (accés a zones o dispositius restringits)

Es poden emprar dades biomètriques per controlar l'accés a determinades zones o dispositius de l'empresa?

Els sistemes de biometria poden ser utilitzats per controlar l'accés a determinades zones, instal·lacions o dispositius (com ordinadors o telèfons) per raons alienes a les obligacions laborals, és a dir, per motius de seguretat, per protegir informació sensible, per impedir l'entrada de persones no autoritzades, etc.

En aquests supòsits, també s'estaria duent a terme un tractament de dades biomètriques i, per tant, s'ha de donar compliment a les previsions establertes en el Reglament General de Protecció de Dades (RGPD):

1. S'ha d'acreditar que el tractament és lícit, és a dir, que concorre una de les condicions establertes a l'article 6 del RGPD, entre les quals es troba: el consentiment de la persona interessada, l'execució d'un contracte, el compliment d'una obligació legal, la protecció d'interessos vitals de la persona interessada o d'una altra, el compliment d'una missió realitzada en interès públic, i la satisfacció d'interessos legítims.

2. S'ha d'alçar la prohibició de tractament que recau sobre les dades biomètriques, assegurant que concorre una de les excepcions de l'article 9 del RGPD, entre les quals hi ha: el consentiment explícit, la protecció d'interessos vitals o l'existència d'un interès públic essencial.

3. S'ha d'acreditar la necessitat i proporcionalitat de la mesura. S'exigeix demostrar que l'objectiu previst no podia assolir-se raonablement de manera igualment eficaç a través d'altres mitjans i que els perjudicis causats no són desproporcionats en relació amb aquest objectiu. D'aquesta manera, l'empresa haurà de demostrar que ha adoptat garanties adequades per reduir l'impacte sobre els drets de les persones interessades.

Aplicant aquestes premisses, un supòsit en el qual l'Agència Espanyola de Protecció de Dades ha considerat adequat a la norma l'ús de sistemes de biometria per controlar l'accés amb finalitats no laborals és el recollit en la consulta prèvia amb referència REGAGE25e00024730156[5]. En aquesta consulta es va entendre que era proporcional i comptava amb base legal i

5 Vegeu: www.aepd.es/documento/regage25e00024730156.pdf

regulació suficient el tractament de dades biomètriques per controlar l'accés a instal·lacions de la Guàrdia Civil. Aquesta argumentació es basa en el fet que es tracta d'instal·lacions sensibles que requereixen d'una especial protecció.

Quines garanties s'han de complir en els sistemes de control d'accessos basats en biometria?

La instal·lació de sistemes biomètrics de control d'accés amb finalitats no laborals pot afectar les persones treballadores que exerceixen les seves tasques a l'interior de les zones protegides. És per això que, en tractar-se de persones interessades, l'empresa o entitat haurà d'informar-los sobre les finalitats per a les quals es fan servir les dades biomètriques; les persones destinatàries de la informació; el termini durant el qual es conservaran les dades biomètriques; la possibilitat d'exercir els drets d'accés, rectificació, supressió, limitació del tractament i portabilitat de les dades; 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).

A més, l'empresa haurà de complir amb els principis relatius al tractament recollits en el Reglament General de Protecció de Dades (art. 5 RGPD) i elaborar una avaluació d'impacte relativa a la protecció de dades.

Quan el tractament de dades personals pugui implicar un alt risc per als drets i llibertats de les persones, l'article 35 del RGPD exigeix la realització d'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[6] aquells «que impliquin l'ús de categories especials de dades a què es refereix l'article 9.1 del RGPD» i aquells «que impliquin l'ús de dades biomètriques amb el propòsit d'identificar de manera única una persona física». En conseqüència, quan l'empresa tracti dades biomètriques haurà de dur a terme l'avaluació d'impacte relativa a la protecció de dades amb caràcter previ a l'inici del tractament, i aquesta haurà d'incloure, almenys:

a. Una descripció sistemàtica de les operacions de tractament previstes i de les finalitats del tractament, inclòs, si escau, l'interès legítim perseguit per la persona responsable del tractament.

b. Una avaluació de la necessitat i la proporcionalitat de les operacions de tractament respecte amb la seva finalitat.

6 Vegeu: https://www.aepd.es/documento/listas-dpia-es-35-4.pdf

c. Una avaluació dels riscos per als drets i llibertats de les persones.

d. Les mesures previstes per afrontar els riscos, incloses garanties, mesures de seguretat i mecanismes que garanteixin la protecció de dades personals, i per demostrar la conformitat amb aquest Reglament, tenint en compte els drets i interessos legítims de les persones interessades i d'altres persones afectades.

Monitoratge i control de l'activitat laboral

Es poden utilitzar dades biomètriques per controlar l'activitat de les persones treballadores?

L'empresa pot adoptar mesures de vigilància i control per verificar el compliment de les obligacions i els deures laborals de les persones treballadores (art. 20.3 ET). En aquest context, hi ha algunes mesures de control que fan ús de la biometria, per exemple, analitzant la veu o les expressions facials, la forma de caminar, la freqüència amb què les persones treballadores escriuen al teclat d'un dispositiu digital, etc.

Aquestes mesures de control no només permeten un monitoratge constant de les persones treballadores, sinó que també atorguen a l'empresa accés a informació addicional –com dades relatives a la salut– que podria afectar de manera substancial els drets fonamentals de les persones titulars de les dades biomètriques.

Per això, per poder instal·lar aquesta tipologia de sistemes de control, en primer lloc, l'empresa haurà de complir amb les obligacions legals que neixen dels diferents textos normatius. S'ha de tenir en compte que:

- La gravació de sons es troba prohibida, excepte per raons de seguretat (art. 89.3 de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals).
- L'ús de sistemes de reconeixement d'emocions es troba prohibit, excepte per motius mèdics o de seguretat (art. 5.1.f) del Reglament d'Intel·ligència Artificial).
- L'ús de dades biomètriques ha de ser lícit, és a dir, ha de complir una de les condicions establertes a l'article 6 del Reglament General de Protecció de Dades (RGPD); i, en el seu cas, ha de superar la prohibició de tractament establerta a l'article 9 del RGPD, és a dir, ha de complir una de les excepcions recollides en aquest article.

- S'ha de realitzar una avaluació d'impacte relativa a la protecció de dades, que ha 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).

A banda de complir amb les obligacions que deriven de la normativa, en segon lloc, tractant-se de sistemes que infereixen en els drets fonamentals de les persones treballadores (p. ex., en el dret a la protecció de dades, en el dret a la intimitat o en el dret a la no discriminació), la mesura de control ha de superar el principi de proporcionalitat, és a dir:

a. ha de ser idònia (susceptible d'aconseguir l'objectiu proposat);

b. ha de ser necessària (que no existeixi una altra mesura més moderada per a la consecució d'aquest objectiu i igual d'eficaç); i

c. ha de ser proporcionada en sentit estricte (que aporti més beneficis per a l'interès general que perjudicis sobre altres béns o valors en conflicte).

Aplicant el principi de proporcionalitat s'haurà d'avaluar, per tant, si existeix un altre sistema menys intrusiu i igual d'eficaç –que un sistema de biometria, en aquest cas– que pugui complir amb la finalitat de control prevista, i si els perjudicis causats pel sistema que es pretén implementar no són desproporcionats en relació amb l'objectiu perseguit.

Tenint en compte la greu ingerència que l'ús de dades biomètriques pot tenir sobre els drets fonamentals de les persones treballadores, difícilment es pot entendre que aquests sistemes de control es troben justificats i superen el principi de proporcionalitat.

Prevenció de riscos laborals

Poden ser tractades les dades biomètriques per vigilar la salut de les persones treballadores?

El Reglament General de Protecció de Dades (RGPD) prohibeix el tractament de dades biomètriques i el tractament de dades de salut amb caràcter general (art. 9.1 RGPD).

Les dades biomètriques són dades personals obtingudes a partir d'un tractament tècnic específic, relatives a les característiques físiques, fisiològiques o conductuals d'una persona física que permeten o confirmen la identificació

única d'aquesta persona (art. 4.14 RGPD). El rostre, l'empremta dactilar, l'iris, la retina, la veu, l'ADN, la manera de caminar o moure's d'una persona podrien quedar incloses dins d'aquesta categoria de dades. Es tracta de dades que es troben estretament vinculades a una persona, atès que inclouen informació de la qual una persona no pot desprendre's amb caràcter general i de la qual, fins i tot, es podria deduir informació sensible relacionada amb la salut de les persones treballadores. A causa de les característiques d'aquestes dades i de la potencial repercussió que la seva utilització pot tenir sobre els drets fonamentals, el Reglament General de Protecció de Dades configura una prohibició de tractament de les dades biomètriques.

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 biomètriques i 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 treballadores. 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 aquesta, per a 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.

A més, 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.

Amb tot això, podrien ser utilitzats controls de biometria per avaluar la salut de les persones treballadores quan hi hagi el consentiment de la persona treballadora o quan es compleixi una de les circumstàncies descrites en la norma, sempre que la mesura no suposi una greu ingerència en els drets fonamentals de la persona treballadora i es trobi justificada. Aquesta justificació podria derivar de les especials condicions del lloc de treball, per exemple, quan es tracti d'instal·lacions amb agents biològics perillosos, on és important identificar ràpidament símptomes d'una possible infecció.

Quines garanties s'han de complir?

Quan s'empri tecnologies de biometria per vigilar la salut de les persones treballadores, l'empresa haurà de complir les següents garanties:

- S'haurà d'informar les persones treballadores sobre les finalitats per a les quals es faran servir les dades biomètriques; les persones destinatàries de la informació; el termini durant el qual es conservaran les dades biomètriques; la possibilitat d'exercir els drets d'accés, rectificació, supressió, limitació del tractament i portabilitat de les dades; 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).
- A més, l'empresa haurà de comunicar a la persona treballadora els resultats de la vigilància de la salut (art. 22.3 LPRL).
- S'haurà d'informar a la RLPT sobre els riscos identificats i les mesures i activitats de protecció i prevenció aplicades (art. 18.1 LPRL), dins de les quals s'englobaria la implementació de controls biomètrics per supervisar la salut.
- A més, haurà de consultar amb la RLPT l'adopció d'aquests sistemes perquè es tracta d'una decisió que pot tenir efectes substancials sobre la seguretat i salut de les persones treballadores (art. 33.1.f) LPRL).
- La mesura ha de superar el principi de proporcionalitat, és a dir, ha de ser idònia, necessària i proporcionada en sentit estricte.
- S'hauran de complir els principis relatius al tractament de dades personals (art. 5 RGPD), incloent el principi de limitació de la finalitat (art. 5.1.b) RGPD). Aquest principi implica que l'empresa no podrà usar la informació amb altres finalitats diferents de la finalitat preventiva.
- A més, la normativa sobre prevenció de riscos laborals reconeix que les dades relatives a la vigilància de la salut no podran ser emprades amb

finalitats discriminatòries ni en perjudici de la persona treballadora (art. 22.4 LPRL).

- El tractament de les dades biomètriques amb aquestes finalitats haurà de ser realitzat per una persona professional subjecta a l'obligació de secret professional o sota la seva responsabilitat (art. 9.3 RGPD).
- L'accés a la informació mèdica quedarà limitat al personal mèdic i a les autoritats sanitàries que realitzin la vigilància de la salut. Per transmetre aquesta informació a la persona empresària o altres persones es requerirà el consentiment exprés de la persona treballadora. No obstant això, sí que podran ser comunicades a l'empresa les conclusions en relació amb l'aptitud de la persona treballadora per exercir el lloc de treball o amb la necessitat d'introduir mesures de protecció i prevenció (art. 22.4 RGPD).

Reconeixement d'emocions

Què són els sistemes de reconeixement d'emocions basats en biometria?

Els sistemes de reconeixement d'emocions són aquells sistemes d'intel·ligència artificial que empren dades biomètriques, com, per exemple, el rostre o la veu, per distingir o inferir les emocions o les intencions de les persones.

Està permès l'ús de biometria per analitzar l'estat emocional de les persones treballadores? Quines excepcions contempla la normativa?

El Reglament d'Intel·ligència Artificial (RIA) prohibeix l'ús de sistemes de reconeixement d'emocions en el lloc de treball; encara que introdueix una excepció: 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. Per exemplificar aquesta distinció, el mateix Reglament d'Intel·ligència Artificial esmenta expressament que seria legal la comercialització de sistemes d'IA que detectin el cansament dels pilots o dels conductors professionals per tal

d'evitar accidents (Considerant 18 RIA). 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 implica que l'empresa no pot utilitzar dades biomètriques per inferir les emocions de les persones treballadores, llevat que la tecnologia s'implanti per raons mèdiques o de seguretat. Tanmateix, fins i tot quan la implantació respongui a aquests motius, l'excepció ha de ser interpretada de manera restrictiva. No queda emparada la introducció de sistemes de reconeixement d'emocions amb la finalitat de controlar el benestar general de les persones treballadores –com ara detectar si pateixen estrès, ansietat o avorriment– quan no existeixi un risc específic que justifiqui aquest monitoratge.

En aquest sentit, la Comissió Europea ha considerat que sí que podria concórrer un risc, per exemple, en entorns on s'utilitzen maquinàries perilloses i un elevat nivell d'estrès pugui comprometre la salut de les persones treballadores[7]. En aquests supòsits excepcionals, l'empresa no podria utilitzar les dades obtingudes amb finalitats diferents, com ara l'avaluació del rendiment de la persona treballadora.

A més a més, l'ús d'aquesta tecnologia podria igualment quedar prohibit per l'aplicació d'altres normes, com el Reglament general de protecció de dades.

7 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: ec.europa.eu/newsroom/dae/redirection/document/118659

Quines obligacions ha de complir l'empresa quan s'instal·la un sistema de reconeixement d'emocions per motius mèdics o de seguretat?

Els sistemes que empren dades biomètriques per reconèixer emocions de les persones treballadores i compleixen una finalitat mèdica o de seguretat són considerats sistemes d'IA d'alt risc (Annex III.1.c) RIA). Aquesta qualificació respon a la naturalesa de les dades biomètriques i als perills que pot comportar el seu tractament. Les dades biomètriques són dades personals relatives a les característiques físiques, fisiològiques o conductuals d'una persona física que permeten o confirmen la identificació única d'aquesta. El rostre, l'empremta dactilar, l'iris, la retina, la veu, l'ADN, la manera de caminar o moure's podrien quedar incloses dins d'aquesta categoria de dades. Es tracta de dades que es troben estretament vinculades a una persona, atès que inclouen informació de la qual una persona no pot desprendre's amb caràcter general i de la qual, fins i tot, es podria deduir informació sensible relacionada amb la salut de les persones treballadores.

Per aquestes raons, els sistemes de reconeixement d'emocions que empren dades biomètriques són considerats sistemes d'IA d'alt risc, la qual cosa implica que l'empresa que decideixi implantar-los, en tant que responsable del desplegament, haurà de complir les següent garanties establertes en el Reglament d'Intel·ligència Artificial (RIA):

- 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 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).
- Complir amb els deures d'informació (art. 26.7 RIA).
- Adoptar mesures per garantir l'alfabetització en matèria d'IA de les persones treballadores (art. 4 i Considerant 20 RIA). 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 més, els sistemes de reconeixement d'emocions basats en l'anàlisi de dades biomètriques exigeixen el compliment de la normativa en matèria de protecció de dades. Les obligacions que neixen del Reglament General de Protecció de Dades (RGPD) són les següents:

- Complir els principis relatius al tractament (art. 5 RGPD), entre els quals es troba el principi de minimització de dades i el principi de limitació de la finalitat. Aquests principis exigeixen que només s'emprin aquelles dades biomètriques que siguin realment necessàries i que es garanteixi que no seran tractades amb finalitats diferents a les inicialment previstes (motius mèdics i de seguretat en aquest cas).
- Acreditar la licitud del tractament (art. 6.1 RGPD) i, si escau, l'aixecament de la prohibició de tractament (art. 9 RGPD).
- Complir amb els deures d'informació (arts. 12-14 RGPD).
- Garantir la seguretat del tractament, aplicant mesures tècniques i organitzatives apropiades a un nivell de seguretat adequat al risc (art. 32 RGPD).
- Realitzar una avaluació d'impacte relativa a la protecció de dades (art. 35 RGPD).

Finalment, el sistema de reconeixement d'emocions haurà de superar el principi de proporcionalitat, en estar en risc el dret fonamental a la protecció de dades de les persones treballadores. 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.

En termes generals, aplicant el principi de proporcionalitat, l'empresa haurà de demostrar que no existeix un altre sistema menys intrusiu i igual d'eficaç –que un sistema de reconeixement d'emocions, en aquest cas– que pugui complir amb la finalitat mèdica o de seguretat prevista, i que els perjudicis causats pel sistema que es pretén implementar no són desproporcionats en relació amb l'objectiu perseguit.

Si s'instal·la un sistema de reconeixement d'emocions, es deriva alguna obligació en matèria de prevenció de riscos laborals?

Quan s'instal·la un sistema de reconeixement d'emocions per raons de seguretat o mèdiques, significa que hi ha un risc detectat que es vol prevenir o reduir amb aquest sistema. Per això, **abans d'instal·lar-lo,** s'ha de fer una **avaluació de riscos** que en justifiqui l'ús i demostri que realment és necessari.

A més, l'empresa té el deure d'informar les persones treballadores i la RLPT, si escau, dels riscos identificats i de les mesures de protecció i prevenció aplicades (art. 18.1 LPRL), dins de les quals s'englobaria la implementació d'un sistema de reconeixement d'emocions.

Igualment, l'empresa haurà de consultar amb la RLPT l'adopció de sistemes de reconeixement d'emocions per motius mèdics o amb finalitats de seguretat, ja que es tracta d'una decisió que pot tenir efectes substancials sobre la seguretat i salut de les persones treballadores (art. 33.1.f) LPRL).

S'ha d'informar les persones treballadores?

Si l'empresa decideix instal·lar un sistema de reconeixement d'emocions, les persones treballadores hauran de ser informades sobre les finalitats del tractament, les persones destinatàries de la informació, el termini durant el qual es conservaran les dades biomètriques, la possibilitat d'exercir els drets d'accés, rectificació, limitació del tractament i supressió, 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). És important remarcar que l'empresa haurà de comunicar, en tot cas, a les persones treballadores que les seves dades personals seran utilitzades per un sistema d'intel·ligència artificial amb un fi determinat; havent d'especificar aquest objectiu d'ús.

Aquest deure d'informació és, a més, reiterat pel Reglament d'Intel·ligència Artificial. En l'article 26.7, s'estableix que l'empresa, abans de posar en servei o utilitzar un sistema d'IA d'alt risc en el lloc de treball, haurà d'informar les persones treballadores afectades que estaran exposades a la utilització de l'esmentat sistema.

Per la seva banda, el Reglament d'Intel·ligència Artificial també reconeix un dret d'explicació (art. 86 RIA). En el supòsit en què l'empresa adopti decisions basades en els resultats d'un sistema de reconeixement d'emocions, 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.

Si el sistema d'IA no empra dades biomètriques en el reconeixement d'emocions, ¿també es considera un sistema d'alt risc?

Hi ha sistemes d'IA que poden reconèixer o deduir emocions a partir d'informació o dades que no són biomètriques i que no són considerades com a sistemes d'alt risc. Dins d'aquesta categoria s'inclouen els sistemes d'IA destinats a interactuar amb persones físiques, com *chatbots* (p. ex., ChatGPT), que poden interpretar com es troba la persona arran de l'anàlisi de les paraules.

En aquests supòsits, el risc d'un impacte negatiu sobre els drets fonamentals de les persones treballadores que interactuen amb els sistemes d'IA disminueix. Per això, les obligacions que ha de complir l'empresa també es veuen reduïdes. No obstant això, igualment l'empresa haurà d'informar del funcionament del sistema a les persones treballadores exposades a ell (art. 50.3 RIA). A més, les entitats proveïdores d'aquesta tipologia de sistemes d'IA tenen l'obligació de garantir que els sistemes estiguin dissenyats de manera que **les persones sàpiguen que estan interactuant amb una IA i no amb un ésser humà** (art. 50.1 RIA).

IA, decisions automatitzades i tractament de dades biomètriques

¿Pot una empresa instal·lar sistemes d'IA que emprin dades biomètriques per categoritzar les persones treballadores atenent la seva raça, opinió política, afiliació sindical, etc.?

El Reglament d'Intel·ligència Artificial prohibeix la utilització 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 que, a partir de biometria, intentin «endevinar» aquestes característiques i classificar les persones treballadores d'acord amb elles.

Pot l'empresa emprar dades biomètriques per prendre decisions automatitzades?

Les decisions individuals automatitzades –que són aquelles en què no hi intervé una actuació humana significativa– 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 quan 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.

Igualment, fins i tot en aquests supòsits en què podria 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, 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 emprar dades biomètriques per prendre decisions automatitzades que afectin les persones treballadores.

Garanties enfront del tractament de dades biomètriques

Quines conseqüències pot tenir un incompliment de la normativa aplicable en l'ús de sistemes de biometria?

Un incompliment de la normativa que regula el tractament de dades biomètriques –p. ex., el seu ús incomplint la prohibició de tractament– pot suposar una vulneració de drets fonamentals, concretament del dret a la intimitat (art. 18.1 CE) i/o del dret a la protecció de dades (art. 18.4 CE). Per això, les persones treballadores, davant d'una potencial lesió dels seus drets fonamentals a causa de la inobservança de la normativa per part de l'empresa, podran presentar demanda de tutela de drets fonamentals expressant els fets que han constituït la vulneració, el dret infringit i la quantia de la indemnització pretesa (arts. 177 i ss LRJS). Igualment, quan la mesura afecti un grup genèric de persones treballadores o un col·lectiu genèric susceptible de determinació individual, els sindicats que tinguin un àmbit d'actuació igual o major al del conflicte també podran iniciar un procediment judicial.

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

- 6.251, per vulneració del dret a la intimitat i a la pròpia imatge (Sentència del Jutjat Social núm. 2 d'Alacant núm. 190/2023, de 15 de setembre de 2023), en haver emprat la imatge de la persona treballadora per a fitxar sense el seu consentiment, sense proporcionar altres opcions per a realitzar el control horari i sense haver realitzat l'avaluació d'impacte relativa a la protecció de dades.

La vulneració de drets fonamentals també pot tenir lloc en l'obtenció de la prova que és utilitzada per l'empresa per acreditar un acomiadament d'una persona treballadora. En aquests supòsits, la persona treballadora podrà presentar demanda per acomiadament, al·legant que la prova ha de ser declarada il·lícita en haver mediat vulneració de drets fonamentals (art. 90.2 LRJS). Si no s'admet la prova i l'empresa no pot provar la infracció comesa per la persona treballadora per altres mitjans, l'acomiadament serà declarat improcedent o nul, depenent de si l'òrgan judicial entén que la lesió de drets fonamentals es projecta també sobre la decisió extintiva. A més, la declaració de nul·litat o improcedència de l'acomiadament pot anar acompanyada del reconeixement d'una indemnització per danys morals.

Pot ser sancionada l'empresa per un incompliment de la normativa en matèria de protecció de dades?

Si l'empresa infringeix la normativa que regula el tractament de dades biomètriques en el lloc de treball, les persones treballadores i/o la representació legal poden denunciar aquesta situació davant les autoritats competents, ja sigui l'Agència Espanyola de Protecció de Dades (o l'Autoritat Catalana de Protecció de Dades) o la Inspecció de Treball i Seguretat Social, depenent de la infracció de què es tracti.

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[8]). 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.
  - 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.

8 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

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. En cas que una empresa s'hagi negat a permetre-li a una persona treballadora, per exemple, l'accés a les seves dades biomètriques, l'autoritat podrà requerir a l'empresa perquè atengui el dret demanat; amb possibilitat d'incórrer en la comissió d'una infracció si no compleix amb la resolució.

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

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

Entre les infraccions que podrien ser sancionades per la ITSS en l'àmbit del tractament de dades biomètriques es troben:

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

- 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.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).

L'ús indegut de dades biomètriques a la feina pot exposar a les empreses a sancions de fins a gairebé un milió d'euros per a l'empresa per vulnerar drets laborals, de privacitat i de prevenció de riscos.

Infraccions en matèria de prevenció de riscos laborals:

- 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 efectuar els reconeixements mèdics i proves de vigilància periòdica de l'estat de salut de les persones treballadores que siguin procedents conforme a la normativa sobre prevenció de riscos laborals, o no comunicar-ne el seu resultat a les persones treballadores afectades (art. 12.2 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).

- Infraccions molt greus que poden ser sancionades amb multa, en el seu grau mínim, de 49.181 a 196.745 euros; en el seu grau mitjà, de 196.746 a 491.865 euros; i en el seu grau màxim, de 491.866 a 983.736 euros (art. 40.2.c) LISOS):

  - Incomplir el deure de confidencialitat en l'ús de les dades relatives a la vigilància de la salut de les persones treballadores, en els termes que preveu l'apartat 4 de l'article 22 de la Llei de Prevenció de Riscos Laborals (art. 13.5 LISOS).

Drets col·lectius davant el control tecnològic

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 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)[9].
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).

9 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).

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).

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).

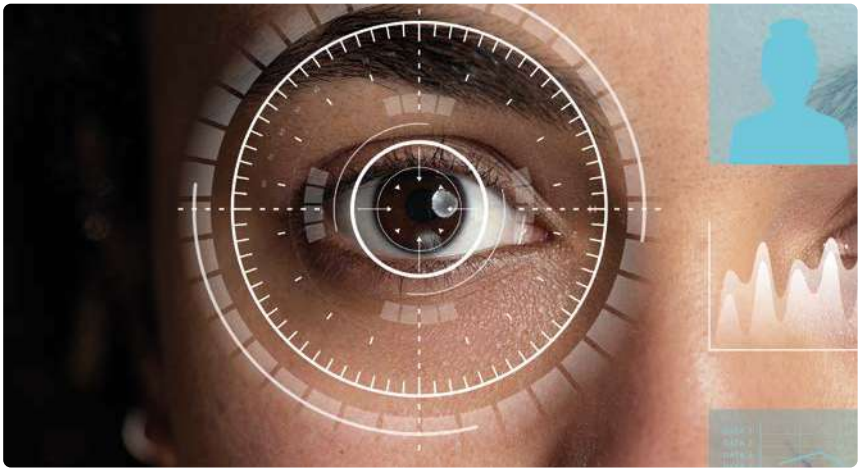
Pot la RLPT acudir a la jurisdicció social davant un incompliment dels drets d'informació i consulta?

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.



Negar informació sobre algoritmes a la representació sindical pot vulnerar la llibertat sindical i comportar la nul·litat de la pràctica empresarial i indemnitzacions.

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 el registre de jornada

Prohibició o limitació estricta de l'ús de dades biomètriques

Els sistemes de registre de jornada que empren tecnologies de biometria (per exemple, sistemes de reconeixement facial o d'escàner d'empremta dactilar) poden ser especialment intrusius perquè recopilen dades sensibles de les persones treballadores (empremta dactilar, veu, rostre, etc.). De fet, segons s'exposa en l'apartat 2.5 de la guia, la normativa sobre protecció de dades prohibeix el tractament de les dades biomètriques amb caràcter general.

El conveni pot adoptar una protecció reforçada prohibint en tot cas i sense excepcions el registre horari mitjançant dades biomètriques. En l'apartat 2.3 de la guia es recullen les mesures de seguretat que l'Agència Espanyola de Protecció de Dades considera que l'empresa hauria de complir en el tractament de dades biomètriques.

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

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 necessàriesper a la salud de la persona treballadora. A més de nou, es molt important que se pacte que qualsevol us de 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.


UGT.cat

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

Sistemes biomètrics

1

UGT.cat