

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

Edició: UGT de Catalunya. Any 2025

Estudi i redacció: Dr. Adrià Todolí Signes, Universitat de València

Amb la col·laboració de

Amb el suport de:



Índex

1. Introducció.....	5
2. Drets individuals en matèria de privacitat i prevenció de riscos laborals .	8
2.1. Davant la videovigilància.....	8
2.1.1. Sistemes de videovigilància amb IA.....	22
2.2. Davant el GPS.....	30
2.3. Davant l'ús de sistemes biomètrics	49
2.3.1. Registre de jornada i control d'accés o presència amb fins laborals	55
2.3.2. Control d'accés amb finalitats no laborals (accés a zones o dispositius restringits)	57
2.3.3. Monitoratge i control de l'activitat laboral	59
2.3.4. Prevenció de riscos laborals	60
2.3.5. Reconeixement d'emocions.....	63
2.3.6. IA, decisions automatitzades i tractament de dades biomètriques	67
2.3.7. Garanties enfront del tractament de dades biomètriques	68
2.4. Davant el registre de l'ordinador i del telèfon mòbil	73
2.5. Davant el registre de jornada	85
2.6. Davant el control algorítmic	99
2.7. Davant les EPIs intel·ligents	113
3. Drets col·lectius davant el control tecnològic	124
4. Recomanacions i estratègies per protegir les persones treballadores	
davant el control tecnològic en la negociació col·lectiva.....	133
4.1. Davant la videovigilància, la gravació de so i el GPS al treball	133
4.2. Davant el registre de dispositius electrònics	139
4.3. Davant el registre de jornada	144
4.4. Davant l'ús de sensors, EPIs intel·ligents i sistemes d'intel·ligència artificial	
149	

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 una realitat futura: 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 treballadors, 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. Ens trobem 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 disputar-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 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 d'UGT Catalunya considerem necessari. Existeixen 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 disputar cada espai en defensa dels drets laborals.

En aquest sentit, des d'UGT Catalunya reivindicuem que els drets fonamentals; la intimitat, la protecció de dades, la salut laboral i la dignitat, han de ser límits infranquejables davant qualsevol innovació tecnològica. No pot existir 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 d'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
UGT de Catalunya

Reyes Solaz García
Secretària Nacional –Salut Laboral
UGT de Catalunya

1. Introducció

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

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

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

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

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

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

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

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

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

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

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

Aquesta guia neix amb aquesta vocació. Està pensada com un instrument pràctic per als delegats i delegades d'UGT Catalunya, així com per a les persones afiliades, amb l'objectiu de facilitar el coneixement dels drets individuals i col·lectius davant el control tecnològic. La guia ofereix exemples concrets dels usos més habituals de la tecnologia

per part de les empreses i analitza, de manera clara i entenedora, quins són els límits legals i sindicals en cada cas.

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

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

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

2. Drets individuals en matèria de privacitat i prevenció de riscos laborals

2.1. Davant la videovigilància

Es poden instal·lar sistemes de videovigilància per controlar l'activitat de les persones treballadores?

La instal·lació de sistemes de videovigilància és una de les mesures de control que l'empresa pot adoptar per verificar que les persones treballadores compleixen amb les seves obligacions i deures laborals. De fet, en la mateixa normativa espanyola sobre protecció de dades (és a dir, en la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD)) es preveu que l'empresa pugui tractar les imatges obtingudes a través de sistemes de càmeres o videocàmeres per a l'exercici de les seves facultats de control i direcció (art. 89 LOPDGDD). No obstant això, la possibilitat d'emprar aquesta eina de control no eximeix l'empresa del compliment d'unes garanties. En aquest sentit, l'empresa, en l'adopció d'un sistema de videovigilància, haurà de tenir en consideració la dignitat de les persones treballadores (art. 20.3 ET), respectar el marc legal existent i els límits que el mateix imposa (art. 89 LOPDGDD) i observar el principi de proporcionalitat.

Es requereix el consentiment de les persones treballadores per instal·lar les càmeres de videovigilància?

Per instal·lar càmeres de videovigilància amb finalitats de control no es requereix el consentiment de les persones treballadores, perquè es tracta d'una mesura que es troba justificada per l'existència d'una relació laboral. Aquesta conclusió, sostinguda per l'Agència Espanyola de Protecció de Dades (en la Guia sobre la protecció de dades en les relacions laborals) sorgeix de l'aplicació del Reglament General de Protecció de Dades (RGPD). D'acord amb aquesta norma, qualsevol tractament de dades personals (com ho són les imatges obtingudes de les càmeres que permeten identificar les persones treballadores) ha de venir justificat per una de les condicions establertes a l'article 6 del RGPD. Entre aquestes condicions es contempla que podran emprar-se dades personals quan el seu tractament sigui "necessari per a executar un contracte en el qual l'interessat és part [...]" (art. 6.1.b) RGPD). En aplicació d'aquest precepte, s'entén que l'exercici de les facultats de direcció i control és necessari per a l'execució del contracte laboral, ja que permet a l'empresa verificar el compliment de les obligacions laborals. Sent que la

instal·lació de sistemes de videovigilància és una de les mesures de control que pot emprar l'empresa, el consentiment, en aquests supòsits, esdevé, per tant, innecessari.

Encara que no es requereixi el consentiment, s'ha d'informar de la seva instal·lació?

Encara que no sigui necessari el consentiment per instal·lar un sistema de videovigilància amb finalitats de control, l'empresa haurà d'informar amb caràcter previ, i de manera expressa, clara i concisa a les persones treballadores sobre aquesta mesura (art. 89.1 LOPDGDD).

Aquest deure d'informació recollit a la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals ha de ser complementat amb el dret d'informació establert al Reglament General de Protecció de Dades (RGPD), concretament als articles 12, 13 i 14. En aquest sentit, el Reglament General de Protecció de Dades indica que la 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, 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 mostri la seva identitat per altres mitjans (art. 12.1 RGPD).

Quina informació s'ha de transmetre a les persones treballadores?

Les persones treballadores hauran de ser informades sobre les finalitats per als quals es faran servir les imatges, inclòs els fins de control; les persones destinatàries de les imatges; el termini durant el qual es conservaran les mateixes (en aquest cas, les gravacions); 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).

Respecte a la informació sobre els drets d'accés, rectificació, supressió i limitació del tractament, ha de ser puntualitzat que, si bé en la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals només es contempla aquesta obligació en la utilització de sistemes de geolocalització (art. 90), es tracta d'un deure d'informació reconegut en el Reglament General de Protecció de Dades (RGPD), per la qual cosa serà aplicable a qualsevol tractament de dades personals, inclòs l'ús de les imatges de les persones treballadores. Aquests drets suposen:

- El dret d'accés a les dades personals (art. 15 RGPD). La persona treballadora podrà demanar a l'empresa que li confirmi si està sent gravada i que li faciliti una còpia de les imatges que han estat captades sobre la seva persona.
- 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 siguin 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 gravacions en les quals apareix la seva imatge. L'empresa estarà obligada a suprimir-les sense dilació indeguda si ja no són necessàries o han estat obtingudes il·lícitament, és a dir, incomplint la normativa. No obstant això, és important tenir en compte que les imatges 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 la seva imatge no sigui utilitzada temporalment per a certes finalitats. L'exercici d'aquest dret implica que l'empresa podrà emmagatzemar les gravacions, però no usar-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.

Si l'empresa no informa que les imatges de la càmera es faran servir per a fins disciplinaris, pot emprar les imatges obtingudes com a prova per sancionar una persona treballadora?

Si l'empresa vol emprar un sistema de videovigilància per controlar l'activitat laboral, en principi, haurà d'informar amb caràcter previ i de manera expressa, clara i concisa les persones treballadores sobre la **finalitat disciplinària** d'aquesta mesura. No obstant això, l'article 89.1, paràgraf segon, de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD) preveu una excepció a aquesta regla. Tot i que les càmeres no hagin estat instal·lades amb finalitats de control laboral, si es capta la comissió flagrant d'un acte il·lícit per les persones treballadores o empleades públiques, l'empresa podrà fer ús d'aquestes gravacions, sempre que s'hagi

col·locat en el lloc de treball el dispositiu a què fa referència l'article 22.4 de la LOPDGDD. Atenent aquest precepte, l'empresa haurà d'haver situat un dispositiu informatiu en lloc prou visible amb la identificació, almenys, de l'existència del tractament, la identitat de la persona responsable i la possibilitat d'exercir els drets que preveuen els articles 15 a 22 del Reglament General de Protecció de Dades, o haver inclòs en el dispositiu informatiu un codi de connexió o adreça d'Internet amb aquesta informació.

Aquesta excepció, que deriva de la jurisprudència constitucional i del Tribunal Suprem (Sentència del Tribunal Constitucional núm. 39/2016, de 3 de març i Sentència del Tribunal Suprem núm. 23/2025, de 14 de gener, entre d'altres), permet, en termes generals, que l'empresa pugui emprar les gravacions obtingudes de càmeres instal·lades per motius aliens al control de les persones treballadores (p. ex., per raons de seguretat), sense necessitat d'haver informat prèviament sobre la seva finalitat disciplinària. Tanmateix, això queda condicionat al fet que es tracti de la comissió flagrant d'un acte il·lícit i que s'hagi instal·lat el dispositiu informatiu referenciat a l'article 22.4 de la LOPDGDD.

Quan s'entén que estem davant la comissió flagrant d'un acte il·lícit?

Quan s'instal·la un sistema de videovigilància per controlar l'activitat laboral, l'empresa ha d'informar expressament sobre la seva existència i finalitat disciplinària a les persones treballadores. No obstant això, la norma preveu una excepció a aquest deure exprés d'informació. Si es capta la comissió flagrant d'un acte il·lícit, podran ser emprades les imatges, encara que no s'hagués informat sobre la finalitat de control del sistema, sempre que s'hagués col·locat el dispositiu informatiu descrit a l'art. 22.4 de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (art. 89.1, paràgraf segon, LOPDGDD).

En primer lloc, respecte a l'expressió "comissió flagrant", s'ha d'entendre que aquesta inclou tant les troballes casuais d'il·lícits laborals, com aquells il·lícits que hagin estat captats després de la revisió de les gravacions davant l'existència de sospites prèvies. D'aquesta manera, l'empresa podrà emprar les gravacions obtingudes de càmeres de seguretat, que no es va informar la seva funció de control laboral, en dos supòsits:

- D'una banda, quan d'un visionat ordinari de les gravacions s'hagi observat un il·lícit comès per una persona treballadora.
- D'altra banda, quan s'hagi efectuat la revisió de les gravacions per corroborar la sospita d'il·lícits laborals que l'empresa mantenia amb caràcter previ. És important assenyalar que, en aquest segon supòsit, la revisió de les gravacions ha d'estar

justificada per l'existència de fundades sospites; és a dir, no quedaria emparada, en principi, una revisió de les gravacions per raons de control quan l'empresa tingui una mera sospita genèrica. Per exemple, no seria adequat revisar les gravacions de les càmeres únicament perquè l'empresa hagi detectat una disminució general de les vendes, sense que existeixin evidències concretes d'irregularitats, com faltes de diners o productes o queixes específiques de clients.

En segon lloc, l'expressió "acte il·lícit" fa referència a aquells incompliments laborals que es troben relacionats amb la seguretat i protecció de les coses o de les persones i que suposen una transgressió de la bona fe contractual (p. ex., manipulació de tiquets (Sentència del Tribunal Suprem núm. 86/2017, d'1 de febrer de 2017) o sostracció de productes (Sentència del Tribunal Suprem núm. 630/2016, de 7 de juliol de 2016)). Aquesta interpretació neix de la jurisprudència del Tribunal Suprem; qui va establir, en la Sentència núm. 77/2017, de 31 de gener de 2017, que la utilització de càmeres per raons de seguretat "inclou la vigilància d'actes il·lícits dels empleats i de tercers i en definitiva de la seguretat del centre de treball però exclou un altre tipus de control laboral que sigui aliè a la seguretat, això és el de l'efectivitat en el treball, les absències del lloc de treball, les converses amb companys, etc.".

Per això, quedaria exclosa la possibilitat d'emprar càmeres de seguretat (sobre les quals no s'ha informat de la finalitat de control) per comprovar el compliment d'obligacions referides a condicions de treball ordinàries, com l'horari de treball o el rendiment de les persones treballadores. La Sentència del Tribunal Superior de Justícia de Canàries de Santa Cruz de Tenerife, núm. 135/2025, de 19 de febrer de 2025 va declarar il·lícita la prova que havia estat obtinguda d'un sistema de videovigilància instal·lat per raons de seguretat, perquè la revisió de les càmeres no venia justificada per la sospita de la comissió d'un acte il·lícit. En aquest cas, la irregularitat comesa per les persones treballadores –deixadesa de les seves funcions laborals per mantenir relacions sexuals en horari de treball– era un acte aliè a la seguretat de les instal·lacions de l'empresa i els seus béns; per la qual cosa per poder emprar les imatges del sistema de videovigilància l'empresa hauria d'haver informat de la seva finalitat de control.

Pot l'empresa utilitzar les càmeres de seguretat, per provar la comissió flagrant d'actes il·lícits, de forma continuada sense informar les persones treballadores sobre la finalitat de control del sistema?

La possibilitat d'emprar càmeres de seguretat per controlar l'activitat laboral de les persones treballadores ha de ser entesa, en principi, com una via excepcional. Si una empresa pretén utilitzar, de forma reiterada, un sistema de videovigilància amb finalitats disciplinàries haurà d'informar d'aquesta finalitat, amb caràcter previ, les persones

treballadores. Altrament, s'estaria incorrent en una irregularitat per no donar compliment a les garanties recollides a l'article 89.1, paràgraf primer, de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD).

A més, convé tenir en compte que, des que es va aprovar la LOPDGDD, les empreses han comptat amb un termini suficient per adaptar l'ús dels seus sistemes de videovigilància als canvis normatius. Sobre aquest punt, es pronuncia el Tribunal Superior de Justícia del País Basc en la seva Sentència núm. 71/2024, de 16 de gener de 2024. Aquesta sentència descriu un supòsit en el qual una empresa havia acomiadat un treballador per robar materials, utilitzant com a prova unes gravacions obtingudes d'una càmera, sobre la qual el treballador no havia estat informat de la seva finalitat de control. El TSJ del País Basc declara la nul·litat de l'acomiadament per vulneració del dret a la intimitat del treballador, en entendre que hi havia hagut un incompliment de la normativa sobre protecció de dades. El Tribunal raona que la previsió excepcional contemplada a l'article 89 de la LOPDGDD és una norma transitòria; puntualitzant que: "si l'empresa no ha utilitzat la via de legalització del sistema per a l'ús de l'activitat dels treballadors no és possible, transcorregut el temps d'inici de la vigència de la llei, el que instrumentalitzi el control per càmeres sense complir la premissa major *[comunicar l'ús de les càmeres com a mesura de control]* que li imposa la llei".

No obstant això, malgrat aquesta sentència, la jurisprudència, generalment, valida la utilització de càmeres, sense haver informat, quan es tracta de la comissió flagrant d'un acte il·lícit, independentment que l'empresa hagi fet ús d'aquesta facultat prèviament amb altres persones treballadores o que hagi transcorregut un termini considerable des de l'aprovació de la LOPDGDD.

Es poden instal·lar càmeres ocultes?

L'article 89 de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals no contempla la possibilitat que l'empresa pugui tractar les imatges obtingudes d'un sistema de videovigilància sense que les persones treballadores tinguin coneixement almenys de la seva existència; ja sigui a través de la transmissió d'informació més detallada o a través de la col·locació d'un dispositiu informatiu.

No obstant això, la jurisprudència –p. ex., en la Sentència del Tribunal Suprem núm. 692/2022, de 22 de juliol– sí que ha legitimat el control ocult en determinats supòsits en què hi havia sospites fundades i raonables de greus irregularitats laborals. En aquests casos, la videovigilància encoberta ha de quedar limitada al temps estrictament necessari

i a l'àrea i la persona treballadora sobre la qual se sostenen les sospites. A més, les imatges han de ser vistes exclusivament per responsables de l'empresa i tractades amb l'únic objectiu de verificar i penalitzar, si escau, la irregularitat laboral. És a dir, en tot cas, s'ha de complir el principi de proporcionalitat.

A banda de les obligacions d'informació, quines altres garanties ha de complir l'empresa?

Independentment que s'hagi informat de la finalitat de control o no, o que es tracti d'una càmera oculta, el sistema de videovigilància que decideixi instal·lar l'empresa ha de respectar, en tot cas, el principi de proporcionalitat. En cas contrari, es podria entendre que la mesura vulnera el dret a la intimitat i/o el dret a la protecció de dades de les persones treballadores afectades. Per comprovar que la mesura és adequada, s'ha de constatar que compleix tres condicions:

- ha de ser idònia, és a dir, susceptible d'aconseguir l'objectiu proposat;
- ha de ser necessària, és a dir, que no existeixi una altra mesura més moderada per a la consecució d'aquest objectiu i igual d'eficaç; i
- ha de ser proporcionada en sentit estricte, és a dir, que aportï més beneficis per a l'interès general que perjudicis sobre altres béns o valors en conflicte.

Atenent aquests requisits, no estaria justificat, per exemple, que l'empresa utilitzés sistemes de videovigilància per controlar les persones treballadores, perquè és la mesura més còmoda o econòmica, si existeixen altres mecanismes de control menys invasius.

A més del principi de proporcionalitat, segons el que disposa el Reglament General de Protecció de Dades (RGPD), quan té lloc un tractament de dades personals s'han de complir els principis relatius al tractament, recollits a l'article 5 del RGPD. Dins d'aquests principis, es troba 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 haurà de ser utilitzada la imatge de les persones treballadores quan la finalitat del tractament d'aquesta dada personal no pugui aconseguir-se raonablement per altres mitjans. Referent a això, l'Agència Espanyola de Protecció de Dades, en la seva Guia sobre la protecció de dades en les relacions laborals, reconeix que, dins de l'àmbit de la videovigilància, aquest principi de minimització de dades exigeix:

- a) "Que el nombre de càmeres es limiti a les necessàries per complir la funció de vigilància"; és a dir, que només s'instal·lin les càmeres que siguin imprescindibles per complir amb l'objectiu previst. D'aquesta manera, si, per exemple, en un

supermercat es pretén controlar que les persones treballadores no manipulin les caixes, les càmeres s'hauran d'instal·lar exclusivament a les zones de cobrament.

- b) "Que el responsable analitzi també els requisits tècnics de les càmeres". És important que l'empresa avaluï les característiques de les càmeres que instal·la per valorar si s'està duent a terme una intrusió desproporcionada en la intimitat de les persones treballadores. Això pot ocórrer quan s'instal·len càmeres que permeten fer zoom o que poden girar-se i captar un ampli camp de visió; podent fins i tot accedir a la visualització de zones de descans.

Així mateix, l'Agència Espanyola de Protecció de Dades destaca la importància de garantir que els monitors de gravació estiguin ubicats en llocs accessibles únicament al personal autoritzat per controlar els equips, evitant en tot cas la seva col·locació en zones on clients o usuaris puguin visualitzar les imatges.

En definitiva, tant el principi de proporcionalitat com el principi de minimització de dades suposen que l'empresa hagi de demostrar que **no hi ha cap altra mesura menys invasiva per als drets fonamentals** de les persones treballadores que permeti controlar l'activitat laboral o demostrar la comissió d'un acte il·lícit. No obstant això, la jurisprudència tendeix a admetre la proporcionalitat dels sistemes de videovigilància, tot i que no s'haja informat les persones treballadores de la seva instal·lació amb finalitats disciplinàries, si el mecanisme compleix amb el seu propòsit.

Es poden gravar sons? En quins supòsits?

Els sistemes de gravació de sons únicament podran ser emprats en el lloc de treball quan existeixin riscos per a la seguretat de les instal·lacions, béns i persones derivats de l'activitat que es desenvolupi en el centre de treball i sempre respectant el principi de proporcionalitat, el d'intervenció mínima i les garanties previstes per a la videovigilància (art. 89.3 LOPDGDD).

D'aquesta manera, per poder instal·lar un sistema de gravació de sons, l'empresa haurà d'acreditar que la seva implementació respon a una finalitat legítima vinculada a la seguretat. A més, haurà de donar compliment al principi de proporcionalitat, és a dir, no podrà ser instal·lat un sistema que no sigui idoni, necessari i proporcionat en sentit estricte, fet que implica que s'haurà d'acreditar que no hi ha cap altra mesura, que pugui complir amb el mateix objectiu, que sigui igual d'eficaç i menys invasiva per als drets fonamentals. En aplicació d'aquestes exigències, amb caràcter general (llevat de raons justificades i necessàries de seguretat, p. ex. les caixes negres dels avions), sembla considerar-se que **la gravació indiscriminada i continuada de la veu no és admissible**. La Sentència del Tribunal Constitucional núm. 98/2000, de 10 d'abril tracta un supòsit en

el qual un casino havia instal·lat micròfons en determinades dependències del lloc de treball (seccions de caixa i ruleta francesa), al·legant que la seva col·locació responia a raons de seguretat per resoldre possibles reclamacions. El Tribunal Constitucional va entendre que aquesta mesura suposava una intromissió il·legítima en el dret a la intimitat perquè permetia l'audició de tota mena de converses, incloses les de les persones treballadores, i perquè resultava desproporcionada en no haver quedat acreditat que la seva instal·lació fos indispensable per a la seguretat i bon funcionament del casino.

Malgrat aquestes exigències, ha de ser recalcat que en l'àmbit d'empreses de *call-centre* o telemàrqueting la jurisprudència sí que sembla admetre la gravació de les converses i trucades efectuades amb els clients per la naturalesa de la prestació del servei (Sentència del Tribunal Suprem de 5 de desembre de 2003, rec. 52/2003).

Es pot instal·lar la videovigilància en qualsevol espai del lloc de treball?

L'article 89.2 de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals prohibeix la instal·lació de sistemes de videovigilància i/o de gravació de sons en aquells llocs destinats al descans o esbargiment de les persones treballadores; és a dir, en aquells llocs on no es desenvolupa la relació laboral, com podrien ser-ho vestuaris, lavabos, menjadors i anàlegs. La col·locació de càmeres de videovigilància o de sistemes de gravació de sons en aquests llocs suposa una vulneració, amb caràcter general, del dret a la intimitat de les persones treballadores.

A més, s'ha arribat a considerar que existia una intromissió il·legítima a aquest dret fonamental quan l'empresa –havent instal·lat videovigilància en àrees des de les quals es podia accedir a la visualització de zones de descans o esbargiment– no va provar que les "càmeres no enfoquessin, o poguessin enfocar amb una manipulació simple" a aquestes àrees de privacitat (Sentència del Tribunal Superior de Justícia de Castella-la Manxa, núm. 1517/2023, de 2 de novembre).

Quin és el termini durant el qual l'empresa pot conservar les gravacions?

L'empresa podrà conservar les gravacions un termini màxim d'un mes des de la seva captació (art. 22.3 en relació amb l'art. 89.3 de la LOPDGDD). Per la qual cosa abans que transcorri aquest termini l'empresa haurà de suprimir les imatges i sons que hagin estat obtingudes mitjançant els sistemes de videovigilància o de gravació de sons. No obstant això, aquest termini podrà ser ampliat quan l'empresa hagi de conservar les gravacions per acreditar la comissió d'actes que atempten contra la integritat de persones, béns o instal·lacions. En aquests supòsits, l'empresa té el deure de posar les gravacions a disposició de l'Agència Espanyola de Protecció de Dades en el termini màxim de 72

hores. Aquest termini es comptabilitza des que l'empresa tingui coneixement de l'existència de la gravació (art. 22.3 de la LOPDGDD).

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

Un incompliment de la normativa que regula l'ús de sistemes de videovigilància en el lloc de treball –p. ex., la instal·lació de càmeres amb gravació de so o la col·locació de videovigilància en llocs de descans– 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 sistemes de videovigilància, en:

- 6.251 euros, per vulneració del dret a la intimitat en haver-se col·locat càmeres en zones dedicades al descans i esbargiment (Sentència del Tribunal Superior de Justícia de Catalunya núm. 2298/2022, de 12 d'abril de 2022 i Sentència del Tribunal Superior de Justícia de Canàries de Las Palmas de Gran Canària núm. 605/2021, de 15 de juny de 2021).
- 26.252 euros, per vulneració dels drets a la integritat física i moral, a la tutela judicial efectiva (garantia d'indemnitat) i a la intimitat (Sentència del Tribunal Superior de Justícia de Catalunya núm. 5064/2019, de 21 d'octubre de 2019). El tribunal va considerar que la instal·lació de càmeres exclusivament a la garita on es trobava la persona treballadora no superava el principi de proporcionalitat, perquè no existia justificació darrere de la seva instal·lació més enllà de pressionar la persona treballadora en un context d'assetjament i conflictivitat que havia estat provat.

- 30.001 euros, per vulneració del dret a la intimitat en haver-se instal·lat un sistema de videovigilància que podia enfocar a zones de privacitat (taquilles, vestuari, accés a banys, menjador social, etc.) (Sentència del Tribunal Superior de Castella-la Manxa núm. 1517/2023, de 2 de novembre de 2023).

La vulneració de drets fonamentals també pot tenir lloc en l'obtenció de la prova que és emprada per l'empresa per acreditar un acomiadament d'una persona treballadora. En aquests supòsits, la persona treballadora podrà presentar demanda per acomiadament, al·legant que la prova ha de ser declarada il·lícita en haver mediat vulneració de drets fonamentals (art. 90.2 LRJS). Si no s'admet la prova i l'empresa no pot provar la infracció comesa per la persona treballadora per altres mitjans, l'acomiadament serà declarat improcedent (entre d'altres, Sentència del Tribunal Superior de Justícia de Canàries de Santa Cruz de Tenerife núm. 135/2025, de 19 de febrer de 2025) o nul (entre d'altres, Sentència del Tribunal Superior de Justícia de Castella i Lleó de Burgos núm. 337/2024, de 2 de maig de 2024); depenent de si l'òrgan judicial entén que la lesió de drets fonamentals es projecta també sobre la decisió extintiva. En alguns supòsits la declaració de nul·litat o improcedència de l'acomiadament ha anat acompanyada del reconeixement d'una indemnització per danys morals:

- 1.500 euros, per vulneració del dret a la protecció de dades en incomplir-se els deures d'informació (Sentència del Tribunal Superior de Justícia de Catalunya núm. 6036/2019, de 13 de desembre de 2019).
- 4.000 euros, per vulneració del dret a la protecció de dades en incomplir-se els deures d'informació (Sentència del Tribunal Superior de Justícia de Catalunya núm. 2842/2019).

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 l'ús de sistemes de videovigilància 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'actuació¹). 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.

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

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

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 gravacions on apareix la seva imatge, 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 sistemes de sistemes de videovigilància 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 de la videovigilància es troben:

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

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

La introducció de sistemes de videovigilància 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 depressió².

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.

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.

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 videovigilància 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 videovigilància 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).

2.1.1. Sistemes de videovigilància amb IA

Amb quines finalitats solen utilitzar-se els sistemes que combinen intel·ligència artificial i videovigilància en els llocs de treball?

La videovigilància en el lloc de treball pot complementar-se amb sistemes d'intel·ligència artificial que analitzen les imatges captades i permeten a l'empresa obtenir informació addicional i identificar patrons o comportaments de les persones treballadores. En l'àmbit laboral, els sistemes que combinen intel·ligència artificial i videovigilància poden tenir múltiples utilitats. Una d'elles respon a l'ús d'aquests sistemes amb finalitats de seguretat i prevenció de riscos laborals; per exemple, per detectar comportaments perillosos, controlar l'ús d'equips de protecció, prevenir accidents, detectar problemes posturals, analitzar la temperatura corporal o actuar davant situacions d'emergència o violència. També es poden utilitzar per controlar l'activitat laboral i avaluar el rendiment o la productivitat de les persones treballadores; analitzant tasques, temps de treball o la

qualitat del servei prestat. Una altra de les utilitats que se li ha atorgat a aquest tipus de sistemes és el reconeixement d'emocions o estats anímics de les persones treballadores, per exemple, mitjançant l'anàlisi del rostre, la veu o el comportament, amb l'objectiu de mesurar el clima laboral, l'estat de salut o la motivació, fins i tot durant processos de selecció de personal.

Ara bé, que la tecnologia pugui emprar-se amb aquestes finalitats no significa que la normativa empari qualsevol ús dels sistemes que combinin IA amb videovigilància.

Quins són els principals riscos que planteja l'ús d'aquesta tipologia de sistemes?

Les càmeres intel·ligents són tecnologies amb una major capacitat d'ingerència en els drets fonamentals, ja que possibiliten un control més exhaustiu sobre les persones treballadores i l'accés a informació sensible. Els riscos derivats de la seva implantació en l'entorn laboral es relacionen, entre altres aspectes, amb els trets característics següents:

- *El tractament de dades biomètriques:* en nombroses ocasions (per exemple, quan s'empren per reconèixer emocions), aquestes tecnologies basen els seus resultats en l'examen d'informació biomètrica (el rostre, la veu, la forma de caminar, etc.). 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.
- *La propagació de pràctiques discriminatòries:* aquesta tipologia de sistemes poden ser emprats per a fins no legítims o ser utilitzats per a un fi diferent del que inicialment es preveia. Això podria ocórrer si, per exemple, una empresa decideix instal·lar un sistema d'IA i videovigilància per reforçar les mesures de prevenció de riscos laborals, però posteriorment empra la informació obtinguda per predir les actituds de les persones treballadores davant una vaga. La possibilitat d'accedir a informació sensible, quan no ve justificada per un fi legítim, pot facilitar la propagació de pràctiques discriminatòries.
- *La presa de decisions automatitzades:* l'ús de sistemes de videovigilància i IA pot donar lloc a la presa de decisions automatitzades basades en els seus resultats. Això es produiria, per exemple, si el sistema decidís sancionar una persona treballadora perquè, segons les dades obtingudes, no compleix els nivells de productivitat exigits. Aquest tipus de decisions es caracteritzen per una manca de transparència, ja que la persona treballadora afectada desconeix el procés seguit i els criteris que han conduït a l'obtenció del resultat.

Aquests riscos s'han tingut en compte en regular l'ús de sistemes d'IA en l'entorn laboral. Atès el potencial impacte de la IA sobre els drets fonamentals de les persones treballadores, la normativa prohibeix determinades pràctiques i estableix garanties reforçades per als supòsits que no es troben dins d'aquestes prohibicions.

Quins sistemes d'IA estan prohibits per la normativa?

Tant el Reglament d'Intel·ligència Artificial (RIA), com el Reglament General de Protecció de Dades (RGPD) prohibeixen la utilització de determinats sistemes d'IA. Dins l'àmbit de la videovigilància, les prohibicions que resulten rellevants són les següents:

- Sistemes de reconeixement d'emocions

Els sistemes de reconeixement d'emocions són aquells sistemes d'IA que empren dades biomètriques, com, p. ex., el rostre o la veu, per distingir o inferir les emocions o les intencions de les persones. El Reglament d'Intel·ligència Artificial prohibeix l'ús d'aquesta tipologia de sistemes 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 RIA 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, dins dels sistemes de videovigilància, implica que l'empresa no pot utilitzar les gravacions efectuades per detectar les emocions de les persones treballadores, tret que la tecnologia s'instal·li per motius mèdics o de seguretat. No obstant això, tot i que la raó de la seva col·locació respongués a motius mèdics o de seguretat, el seu ús podria estar prohibit per l'aplicació d'altres textos normatius, com el Reglament General de Protecció de Dades.

- Sistemes que dedueixin informació sensible

El Reglament d'Intel·ligència Artificial prohibeix igualment 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 les imatges que obtinguin de les

càmeres, intentin "endevinar" aquestes característiques i classificar les persones treballadores d'acord amb elles.

El Reglament d'Intel·ligència Artificial pretén evitar la propagació de pràctiques discriminatòries; que podrien tenir lloc si, per exemple, una empresa instal·la un sistema d'IA i captació d'imatges per reconèixer quines persones treballadores tenen més probabilitat d'exercir el seu dret a vaga o afiliar-se a un sindicat.

- Tractament de dades biomètriques segons el Reglament General de Protecció de Dades

Qualsevol tractament de dades biomètriques, al marge que la normativa –el Reglament d'Intel·ligència Artificial– prohibeixi determinats usos concrets, ha d'observar el Reglament General de Protecció de Dades (RGPD). El RGPD qualifica les dades biomètriques dirigides a identificar una persona com a dades especialment sensibles, és a dir, com a dades que requereixen una major protecció; i per això prohibeix el seu tractament amb caràcter general. Això implica que només podran ser utilitzades càmeres que analitzin la biometria de les persones treballadores 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 dades biomètriques dirigides a identificar a la persona. A més, la normativa europea tampoc permet la presa de decisions individuals automatitzades basades en dades biomètriques, en tractar-se d'una categoria especial de dades personals (art. 22.4 RGPD).

Què succeeix amb la resta de les pràctiques d'IA que no estan prohibides?

Els sistemes que combinin IA i captació d'imatges i que no estiguin expressament prohibits per la normativa hauran d'observar les obligacions i garanties recollides tant en el Reglament d'Intel·ligència Artificial (RIA) com en el Reglament General de Protecció de Dades (RGPD) i superar, a més, el principi de proporcionalitat.

- Obligacions recollides en el Reglament d'Intel·ligència Artificial

El Reglament d'Intel·ligència Artificial 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'indole laboral o la promoció o rescissió de relacions contractuals d'indole 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 s'integrarien, per tant, aquells sistemes que utilitzen IA i captació d'imatges i que siguin emprats per donar suport a la presa de decisions relacionades amb la gestió de recursos humans o la productivitat de l'empresa.

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 d'obligacions, entre les quals es troben: adoptar mesures tècniques i organitzatives adequades per garantir que s'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); així com, complir amb els deures d'informació (art. 26.7 RIA).

- Obligacions recollides en el Reglament General de Protecció de Dades

D'altra banda, el Reglament General de Protecció de Dades imposa diverses obligacions que l'empresa ha de complir quan utilitzi sistemes de videovigilància que integrin IA. En primer lloc, ha de respectar els principis relatius al tractament establerts a l'article 5 del RGPD i garantir el compliment dels deures d'informació previstos als articles 12 a 14. Així mateix, cal assegurar la licitud del tractament, de manera que no podran tractar-se

les imatges de les persones treballadores si no concorre alguna de les condicions de l'article 6.1 del RGPD i, si és el cas, de l'article 9.2.

Igualment, 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 avaluació³ aquells "que impliquin la utilització de noves tecnologies", entre els quals es trobarien els sistemes d'IA que analitzen imatges captades per càmeres. En conseqüència, l'empresa 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.
- Superació del principi de proporcionalitat

Finalment, el sistema que integri IA i captació d'imatges 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 que integri IA i captació d'imatges– que pugui complir amb la finalitat prevista, i si els perjudicis causats pel

³ Vegeu: <https://www.aepd.es/documento/listas-dpia-es-35-4.pdf>

sistema que es pretén implementar no són desproporcionats en relació amb l'objectiu perseguit.

En definitiva, totes les obligacions descrites i principalment el fet que l'empresa hagi d'acreditar que el sistema de videovigilància que empra IA és realment proporcionat dificulta, de manera significativa, la seva implementació en els llocs de treball. Tot i que sembla admetre's la seva aplicació en alguns supòsits en què es destina a donar compliment a la normativa de prevenció de riscos laborals i millorar la seguretat i benestar de les persones treballadores en els llocs de treball.

S'ha d'informar les persones treballadores?

Si s'instal·la en el lloc de treball un sistema que combina videovigilància i IA, l'empresa ha d'informar les persones treballadores amb caràcter previ, i de manera expressa, clara i concisa sobre aquesta mesura (art. 89.1 LOPDGDD). Aquest deure d'informació recollit a la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals ha de ser complementat amb el dret d'informació establert al Reglament General de Protecció de Dades (RGPD), concretament als articles 12, 13 i 14. En aquest sentit, el RGPD matisa que la 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).

Pel que fa al contingut de la comunicació, 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 personals (en aquest cas, les gravacions), 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-hi 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.

Quina informació s'haurà de transmetre quan l'empresa prengui decisions automatitzades?

Les decisions individuals automatitzades –que són aquelles en què no hi intervé una activitat 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 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.

Partint d'aquesta base, el Reglament General de Protecció de Dades preveu uns deures d'informació específics que han de ser complerts davant la presa de decisions automatitzades. En aquests supòsits, l'empresa, addicionalment, haurà de transmetre a les persones treballadores informació significativa sobre la lògica aplicada, així com la importància i les conseqüències previstes d'aquest tractament per a la persona treballadora (arts. 13.2.f) i 14.2.g) RGPD).

A banda del dret d'informació, quins altres drets tenen les persones treballadores quan s'empren càmeres amb IA?

El Reglament General de Protecció de Dades (RGPD) preveu unes garanties addicionals al dret d'informació respecte a la presa de decisions automatitzades. Quan es prengui una decisió a partir dels resultats del sistema d'IA 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).

Per la seva banda, el Reglament d'Intel·ligència Artificial (RIA) 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 d'IA d'alt risc que utilitzi imatges (i 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.

A més, en aquelles empreses en les quals les persones treballadores es vegin afectades per l'ús de sistemes d'IA, s'hauran 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.

2.2. Davant el GPS

Quan parlem de sistemes de geolocalització, ¿ens referim exclusivament a sistemes de GPS instal·lats en vehicles?

Els sistemes de geolocalització, encara que solen relacionar-se amb l'ús de vehicles, constitueixen una eina de control que pot integrar-se també en altres elements o dispositius utilitzats per les persones treballadores. Principalment, els sistemes de geolocalització o GPS poden trobar-se incorporats a:

- Vehicles o altres mitjans de transport.
- Dispositius electrònics, com tauletes tàctils, ordinadors portàtils o telèfons mòbils.
- Aparells electrònics portàtils que són vestits per les mateixes persones treballadores (*wearable devices*), com polseres, rellotges, ulleres o roba intel·ligent.

Es tracta d'una tecnologia que, a banda de proporcionar informació relativa a la ubicació d'aquests dispositius (i, per tant, de les persones treballadores que els utilitzen), poden aportar a les empreses informació addicional sobre el trajecte realitzat, el temps invertit en cada tasca exercida, la velocitat de conducció, etc.

Es consideren dades personals la informació relativa a la localització?

Els sistemes de geolocalització són instal·lats en elements o dispositius mòbils (vehicles, tauletes tàctils, ordinadors, etc.) que són utilitzats per les persones treballadores. Aquests sistemes no solament permeten conèixer on es troba localitzat el dispositiu, sinó que aporten informació relativa a la ubicació, el temps destinat en els desplaçaments, la forma de conduir, etc. de la persona treballadora que està fent ús d'aquest dispositiu. Per això, quan l'ús d'aquests equips pot vincular-se a una persona treballadora concreta, l'activació del sistema de geolocalització implica el tractament de dades personals (Sentència de l'Audiència Nacional núm. 13/2019, de 6 de febrer de 2019). En conseqüència, els tribunals, amb caràcter general, han assenyalat que, en aquests supòsits, l'ús de sistemes de geolocalització pot incidir potencialment en el dret a la intimitat i en el dret a la protecció de dades de les persones treballadores, per la qual cosa la seva utilització s'ha d'ajustar a les garanties establertes en la normativa en matèria de protecció de dades (Sentència del Tribunal Superior de Castella-la Manxa núm. 487/2015, de 28 d'abril de 2015; o Sentència del Tribunal Superior de Justícia del Principat d'Astúries núm. 3058/2017, de 27 de desembre de 2017).

No obstant això, és rellevant tenir en consideració que alguns tribunals han entès que l'ús d'aquests sistemes no afecta la intimitat de les persones treballadores, argumentant que només proporcionen informació relativa a la ubicació física del vehicle i no a característiques personals dels qui els utilitzen (Sentència del Tribunal Superior de Justícia de Madrid núm. 180/2021, de 24 de febrer de 2021; o Sentència del Tribunal Superior de Justícia de Castella i Lleó de Valladolid, de 27 de juliol de 2023, rec. 350/2023).

Es pot instal·lar un sistema de geolocalització per controlar l'activitat de les persones treballadores?

La instal·lació de sistemes de geolocalització és una de les mesures de control que l'empresa pot adoptar per verificar que les persones treballadores compleixen amb les seves obligacions i deures laborals. De fet, en la normativa espanyola sobre protecció de dades (és a dir, en la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals) es preveu que l'empresa pugui tractar les dades obtingudes a través de sistemes de geolocalització per a l'exercici de les seves funcions de control (art. 90 LOPDGDD). No obstant això, la possibilitat d'emprar aquesta eina de control no eximeix l'empresa del compliment d'unes garanties. En aquest sentit, l'empresa, en l'adopció d'un sistema de geolocalització, haurà de tenir en consideració la dignitat de les persones treballadores (art. 20.3 ET), respectar el marc legal existent i els límits inherents al mateix (art. 90 LOPDGDD) i observar el principi de proporcionalitat.

Es pot emprar un sistema de GPS per registrar la jornada?

L'Estatut dels Treballadors recull el deure de les empreses de garantir el registre diari de jornada (art. 34.9 ET). La normativa laboral vigent no imposa una forma expressa de dur a terme aquest registre; simplement estableix que s'haurà d'incloure l'horari concret d'inici i finalització de la jornada de treball de cada persona treballadora (art. 34.9 ET). Aquestes exigències es complementen, a més, amb el que disposa el Tribunal de Justícia de la Unió Europea, en la seva Resolució de 14 de maig de 2019 (assumpte C-55/18), en la qual es va establir que el sistema de registre havia de ser, en tot cas, objectiu, fiable i accessible. Atenent aquestes exigències, els sistemes de geolocalització podrien ser un mitjà vàlid per al compliment de l'obligació de control horari. No obstant això, en produir-se un tractament de dades personals i veure's afectats els drets fonamentals a la intimitat i a la protecció de dades, en la seva utilització s'haurà d'observar el principi de proporcionalitat, i els principis de minimització i limitació de la finalitat recollides en el Reglament General de Protecció de Dades.

- D'una banda, el principi de proporcionalitat implica que solament podrà emprar-se un sistema de geolocalització per registrar la jornada quan sigui realment necessari per les característiques de l'activitat laboral: per exemple, en supòsits en què el treball es realitza fora de les dependències de l'empresa.
- D'altra banda, segons el que disposa l'Agència Espanyola de Protecció de Dades, en la Guia sobre la protecció de dades en les relacions laborals, els principis de minimització i limitació de la finalitat suposen que el tractament de les dades de geolocalització haurà de quedar reclus al compliment de l'obligació legal de registre. En altres paraules, es podrà comprovar la ubicació de la persona treballadora exclusivament en aquells moments en què s'iniciï o finalitzi la jornada laboral; quedant injustificat l'accés a les dades de geolocalització durant la totalitat de la durada d'aquesta.

És necessari el consentiment de les persones treballadores per instal·lar un sistema GPS?

Per instal·lar un sistema de geolocalització amb finalitats de control no es requereix el consentiment de les persones treballadores, perquè es tracta d'una mesura que es troba justificada per l'existència d'una relació laboral. Aquesta conclusió, sostinguda per l'Agència Espanyola de Protecció de Dades (en la Guia sobre la protecció de dades en les relacions laborals), sorgeix de l'aplicació del Reglament General de Protecció de Dades (RGPD). Qualsevol tractament de dades personals (com ho són les dades de geolocalització que permeten identificar les persones treballadores) ha de venir justificat per una de les condicions establertes a l'article 6 del RGPD. Entre aquestes condicions es contempla que podran emprar-se dades personals quan el seu tractament sigui "necessari per executar un contracte en el qual l'interessat és part [...]" (art. 6.1.b) RGPD). En aplicació d'aquest precepte, s'entén que l'exercici de les facultats de direcció i control és necessari per a l'execució del contracte laboral, ja que permet a l'empresa verificar el compliment de les obligacions laborals. Sent que la instal·lació de sistemes de geolocalització és una de les mesures de control que pot emprar l'empresa, el consentiment, en aquests supòsits, esdevé, per tant, innecessari.

S'ha d'informar les persones treballadores de la seva instal·lació?

Amb caràcter previ a la instal·lació d'un sistema de geolocalització, l'empresa haurà d'informar de manera expressa, clara i inequívoca a les persones treballadores i empleades públiques sobre l'existència i característiques d'aquests dispositius i la finalitat per a la qual seran utilitzats, és a dir, si es faran servir amb finalitats disciplinàries (art. 90.2 LOPDGDD i art. 14 RGPD). Aquest deure d'informació recollit a la Llei Orgànica 3/2018,

de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals ha de ser complementat amb el dret d'informació establert al Reglament General de Protecció de Dades (RGPD), concretament als articles 12, 13 i 14. El RGPD estableix que la 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, haurà de ser facilitada per escrit o per altres mitjans, inclusivament, si escau, per mitjans electrònics. La informació només podrà ser facilitada verbalment quan ho sol·liciti la persona interessada –en aquest cas, la persona treballadora– i sempre que es demostrï la seva identitat per altres mitjans (art. 12.1 RGPD).

Quina informació s'ha de transmetre?

D'acord amb la normativa espanyola sobre protecció de dades, les persones treballadores hauran de ser informades sobre l'existència i característiques dels dispositius de geolocalització. Igualment, l'empresa haurà d'informar-los sobre el possible exercici dels drets d'accés, rectificació, limitació del tractament i supressió (art. 90.2 LOPDGDD).

El contingut del deure d'informació ha de ser completat, a més, amb el que disposa el Reglament General de Protecció de Dades (RGPD). La normativa europea preveu que les persones treballadores hauran de ser informades sobre les finalitats per a les quals es fa servir el GPS, la qual cosa inclou la seva finalitat disciplinària; les persones destinatàries de la informació; el termini durant el qual es conservaran les dades personals (en aquest cas, les dades de geolocalització); la possibilitat d'exercir els drets d'accés, rectificació, supressió i limitació del tractament (previsió que també es contempla a la LOPDGDD); 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).

Els drets d'accés, rectificació, supressió i limitació del tractament suposen:

- El dret d'accés a les dades personals (art. 15 RGPD). La persona treballadora podrà demanar a l'empresa que li confirmi si està sent registrada la seva ubicació i que li faciliti una còpia de les dades de localització que estan sent tractades sobre la seva persona.
- 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 siguin 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 seves dades de localització. L'empresa estarà obligada a suprimir-les sense dilació indeguda si ja no són necessàries o han estat obtingudes 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 la seva ubicació no sigui utilitzada 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.

Si el conveni col·lectiu preveu la possibilitat d'instal·lar sistemes de geolocalització, s'entenen complertes les exigències d'informació?

Aplicant el 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, l'empresa ha d'informar de manera individualitzada, expressa, clara i concisa a les persones treballadores sobre l'existència del sistema de geolocalització, les seves característiques i la finalitat per a la qual ha de ser emprat; tenint en compte que l'incompliment d'aquestes obligacions pot suposar una vulneració del dret a la intimitat i/o del dret a la protecció de dades.

La configuració del deure d'informació impedeix, en principi, considerar que aquest es compleix únicament pel fet que el conveni col·lectiu aplicable contempli la possibilitat d'utilitzar sistemes de geolocalització. No obstant això, en alguns supòsits, els tribunals han considerat que no existia vulneració del dret a la intimitat i/o del dret a la protecció de dades quan, tot i que l'empresa no havia facilitat la informació exigida de forma individualitzada i expressa, la utilització de sistemes de geolocalització estava prevista en el conveni col·lectiu aplicable (Sentència del Tribunal Superior de Justícia d'Andalusia núm. 1662/2023, de 21 de setembre de 2023).

És lícita la prova obtinguda del sistema de geolocalització per sancionar una persona treballadora si no s'han complert els deures d'informació?

D'acord amb la normativa en matèria de protecció de dades, l'empresa ha d'informar les persones treballadores sobre l'existència, les característiques dels sistemes de geolocalització i la finalitat per a la qual seran utilitzats (art. 90.2 LOPDGDD i art. 14 RGPD). Aquests deures d'informació formen part del nucli essencial del dret a la protecció de dades, per la qual cosa un incompliment d'aquestes obligacions per part de l'empresa pot suposar una vulneració de drets fonamentals (Sentència del Tribunal Superior de Justícia de Madrid núm. 763/2019, de 12 de juliol de 2019).

Per aquesta raó, la prova adquirida de les dades d'un sistema de geolocalització sobre el qual no s'ha informat les persones treballadores, amb caràcter general, s'entendrà il·lícita en haver mediat una lesió de drets fonamentals en la seva obtenció (art. 90.2 LRJS). La principal conseqüència que una persona treballadora sigui acomiadada i l'única prova que acredita la comissió de l'incompliment laboral sigui il·lícita, és la declaració de la improcedència (Sentència del Tribunal Superior de Justícia de Canàries núm. 62/2023, de 18 de gener de 2023; Sentència del Tribunal Superior de Justícia de Castella-la Manxa núm. 487/2015, de 28 d'abril de 2015; Sentència del Tribunal Superior de Justícia de Madrid, núm. 260/2014, de 21 de març de 2014); o nul·litat de l'acomiadament (Sentència del Tribunal Superior de Justícia de Madrid núm. 432/2021, de 14 de juny de 2021; Sentència del Tribunal Superior de Justícia de Catalunya núm. 2713/2025, de 15 de maig de 2025).

I si s'ha informat sobre la seva instal·lació, però no sobre les finalitats de control?

L'empresa té el deure d'informar les persones treballadores sobre l'existència i les característiques dels sistemes de geolocalització que són instal·lats en dispositius utilitzats per les mateixes (art. 90.2 LOPDGDD). El deure d'informació inclou també l'obligació de comunicar quina és la finalitat per a la qual seran emprades les dades que s'obtenen del sistema de geolocalització (art. 14 RGPD). Per tant, l'empresa haurà de comunicar expressament a les persones treballadores que el sistema podrà ser utilitzat per controlar l'activitat laboral i aplicar mesures disciplinàries en cas d'irregularitats, si aquesta és la funció que pretén atorgar-li.

El dret de la persona treballadora a ser informada sobre qui posseeix les dades i amb quina finalitat forma part del nucli essencial del dret a la protecció de dades, per la qual cosa un incompliment de les exigències d'informació pot suposar una vulneració de drets fonamentals. En conseqüència, si l'empresa empra les dades obtingudes del sistema de

geolocalització per sancionar una persona treballadora sense haver informat sobre les seves finalitats de control, la prova utilitzada podria ser considerada il·lícita –en aplicació de l'article 90.2 de la Llei Reguladora de la Jurisdicció Social– a l'haver mediat una violació de drets fonamentals en la seva obtenció (Sentència del Tribunal Superior de Justícia de Madrid núm. de 21 de març de 2014; o Sentència del Tribunal Superior de Justícia de Castella-la Manxa núm. 487/2015, de 28 d'abril de 2015).

No obstant això, cal esmentar que en alguns supòsits s'ha considerat vàlid l'ús de la informació extreta del GPS, tot i no haver informat de forma expressa i concreta de la possibilitat d'activar el règim disciplinari, quan de la informació transmesa se'n derivava aquesta conclusió. Aquest és el cas de la Sentència del Tribunal Superior de Justícia de Madrid núm. 236/2025, d'11 de març de 2025, on s'havia informat la persona treballadora, en les clàusules addicionals del contracte de treball, que les dades derivades del dispositiu geolocalitzador instal·lat en el vehicle podien ser tractades per a la: "elaboració de patrons de conducta de conducció per assegurar la seguretat de les persones passatgeres i prendre decisions sobre rendiment i complir obligacions legals, entre elles, gestionar sancions administratives, particularment de la DGT, del conveni i del contracte".

Finalment, és important ressaltar que la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals no preveu respecte dels sistemes de geolocalització –a diferència del que passa amb la videovigilància (art. 89.1 LOPDGDD)– la possibilitat d'emprar aquestes eines per provar la comissió flagrant d'un acte il·lícit, tot i que no hi hagi hagut informació expressa sobre la finalitat del sistema. No obstant això, alguns tribunals consideren que sí que podria ser aplicada aquesta previsió per analogia; és a dir, que prenent com a referència la regulació sobre videovigilància es podria admetre una reducció de les exigències d'informació quan s'estigui davant la comissió flagrant d'un acte il·lícit (Sentència del Tribunal Superior de Justícia de Catalunya núm. 982/2021, de 17 de febrer de 2021).

Es pot estendre el control fora de la jornada laboral?

En principi no es pot emprar un sistema de geolocalització per controlar l'activitat de les persones treballadores i conèixer la seva ubicació quan finalitza la jornada de treball. Això es deu al seu que l'exercici de les facultats empresarials de direcció i control ve justificat per l'existència d'una relació laboral. Per tant, fora del temps de treball, l'empresa no té legitimació per accedir a la informació proporcionada pel sistema de geolocalització. Per poder tractar aquesta informació es requeriria el consentiment de les persones treballadores; el qual difícilment és considerat vàlid a causa de la desigualtat contractual existent en les relacions laborals.

En definitiva, si s'accedeix a les dades proporcionades pel sistema de geolocalització en trams horaris aliens a la jornada laboral, es podria considerar vulnerat el dret a la intimitat i/o el dret a la protecció de dades de la persona treballadora afectada.

No obstant això, el Tribunal Suprem, en la seva Sentència núm. 766/2020, de 15 de setembre de 2020, va considerar proporcionat l'accés a les dades de geolocalització d'un vehicle fora de la jornada laboral per acreditar que la persona treballadora havia emprat l'equip amb finalitats particulars. El Tribunal Suprem va entendre que no s'havia vulnerat el dret a la protecció de dades ni el dret a la intimitat de la persona treballadora, tot i que no se l'havia informat que podia ser emprada la informació amb finalitats disciplinàries, ja que tenia coneixement que no podia utilitzar el vehicle fora de la jornada de treball. És important recalcar, no obstant això, que aquesta sentència no va aplicar la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, que obliga expressament les empreses a informar sobre l'existència i característiques del sistema de geolocalització, per tractar-se d'uns fets anteriors a la seva entrada en vigor.

Si es permet l'ús per a finalitats privades del vehicle d'empresa, quines garanties ha d'introduir l'empresa?

En principi, l'empresa únicament pot accedir a la informació proporcionada pel sistema de geolocalització durant la jornada de treball. No obstant això, sorgeixen dubtes respecte a l'aplicació d'aquesta premissa quan l'empresa ha prohibit expressament l'ús del dispositiu fora del temps de treball.

En aquest sentit, el Tribunal Suprem, en la seva Sentència núm. 766/2020, de 15 de setembre de 2020, va considerar legítim l'ús de les dades de geolocalització obtingudes fora de l'horari laboral per acreditar que la persona treballadora havia utilitzat el vehicle de l'empresa amb finalitats personals, existint una prohibició expressa de fer-ho una vegada finalitzada la jornada.

Ara bé, la sentència del Tribunal Suprem es refereix a un supòsit en què la persona treballadora no estava autoritzada a fer servir el dispositiu fora de l'horari laboral. Per contra, quan la persona treballadora sí que disposa d'autorització per utilitzar el dispositiu en el qual s'integra el sistema de geolocalització (ja sigui un vehicle, un telèfon mòbil, etc.) amb finalitats privades, l'empresa haurà de garantir amb certesa que aquest sistema no estigui operatiu en concloure la jornada laboral (Sentència del Tribunal Superior de Justícia del Principat d'Astúries núm. 3058/2017, de 27 de desembre de 2017).

Sobre aquest punt, l'Agència Espanyola de Protecció de Dades, estableix a la Guia sobre la protecció de dades en les relacions laborals, que una de les mesures que pot adoptar

l'empresa per garantir el compliment de la normativa és proporcionar una exclusió voluntària; és a dir, atorgar a la persona treballadora la facultat de desactivar temporalment el sistema de seguiment. Aquesta possibilitat impediria que l'empresa pugui accedir a informació personal de les persones treballadores fora de la jornada de treball.

Pot l'empresa accedir a la informació fora de l'horari de treball per a finalitats alienes al control de la seva activitat?

Quan les persones treballadores tenen autoritzat l'ús dels dispositius o vehicles –que porten incorporat el sistema de geolocalització– fora de la jornada de treball per a finalitats particulars, l'empresa ha de garantir la desactivació del sistema per tal de respectar la privacitat de les persones treballadores.

En aquests supòsits, resulta complex trobar una justificació, és a dir, una base jurídica que permeti a les empreses accedir a les dades de localització un cop finalitzat l'horari de treball. No obstant això, l'Agència Espanyola de Protecció de Dades, en la Guia sobre la protecció de dades en les relacions laborals, entén que poden existir circumstàncies en les quals l'empresa tingui legitimació per a això, posant com a exemple la prevenció de robatori del vehicle. En tot cas, l'Agència Espanyola de Protecció de Dades recorda que, si s'acredita l'existència d'una base jurídica, el mitjà d'accés a les dades ha de ser proporcionat; per exemple, permetent visualitzar la localització exclusivament quan el vehicle surti d'una àrea o regió predeterminada i no de forma continuada.

A banda de les obligacions d'informació quines altres garanties ha de complir l'empresa?

A banda de complir amb els deures d'informació, l'empresa haurà de garantir que el sistema de geolocalització respecta, en tot cas, el principi de proporcionalitat; altrament, es podria entendre que la mesura vulnera el dret a la intimitat i/o el dret a la protecció de dades de les persones treballadores afectades. Per comprovar que el sistema és adequat, s'ha de constatar que compleix tres condicions:

- ha de ser idoni, és a dir, susceptible d'aconseguir l'objectiu proposat;
- ha de ser necessari, és a dir, que no existeixi una altra mesura més moderada per a la consecució d'aquest objectiu i igual d'eficaç; i
- ha de ser proporcionat en sentit estricte, és a dir, que aportï més beneficis per a l'interès general que perjudicis sobre altres béns o valors en conflicte.

Complementàriament al principi de proporcionalitat, també s'hauran de complir els principis relatius al tractament de dades personals disposats a l'article 5 del Reglament

General de Protecció de Dades (RGPD). Dins d'aquests principis, es troba, d'una banda, el principi de minimització de dades, que exigeix que les dades emprades siguin adequades, pertinents i limitades al 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 de localització 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).

Aplicant el principi de proporcionalitat i els principis de minimització de dades i limitació de la finalitat, l'empresa haurà de provar que el sistema de geolocalització és realment necessari per al compliment de la finalitat prevista, que no existeix un altre mitjà menys invasiu que compleixi amb aquesta finalitat i que les dades obtingudes no són destinades amb un altre objectiu diferent per al qual inicialment van ser recaptades. D'aquesta manera, alguns exemples en els quals es podria entendre incomplerts aquests principis són els següents:

- Quan l'empresa exigeix a les persones treballadores que aportin dispositius de la seva propietat per instal·lar un sistema de geolocalització (Sentència de l'Audiència Nacional núm. 13/2019, de 6 de febrer de 2019).
- Quan l'empresa empra un sistema de geolocalització per controlar l'horari de treball i el sistema recapta les dades de localització de la totalitat de la jornada (AEPD, Guia sobre la protecció de dades en les relacions laborals).
- Quan el sistema de geolocalització continua actiu un cop finalitzada la jornada laboral i la persona treballadora pot emprar el dispositiu amb finalitats privades.
- Quan l'empresa atorga a les persones treballadores un telèfon mòbil que incorpora un acceleròmetre i un sistema GPS, que proporciona informació sobre el moviment i la ubicació de forma continuada (Sentència del Tribunal Superior de Justícia de Catalunya núm. 3613/2013, de 23 de maig de 2013). En aquest cas particular, a més, les persones treballadores no podien desactivar el sistema i s'havien de portar el telèfon mòbil a les seves respectives cases per carregar la bateria.

Es pot exigir a la persona treballadora que porti el seu propi dispositiu per instal·lar un sistema de geolocalització?

No és lícit que l'empresa exigeixi unilateralment a les persones treballadores que aportin mitjans de la seva propietat, com un telèfon mòbil o un ordinador, per instal·lar una aplicació que permeti conèixer la seva localització. Aquest criteri va ser sostingut per

l'Audiència Nacional, en la seva Sentència núm. 13/2019, de 6 de febrer de 2019, que va ser posteriorment confirmada per la Sentència del Tribunal Suprem núm. 163/2021, de 8 de febrer de 2021.

L'Audiència Nacional va declarar la nul·litat d'una mesura empresarial que obligava les persones treballadores amb categoria de repartidor/a a aportar un telèfon mòbil, amb connexió a internet i de la seva propietat, i a instal·lar-hi una aplicació informàtica de l'empresa que permetia conèixer la geolocalització de la persona treballadora. Es va considerar que aquesta mesura era contrària al dret a la protecció de dades de les persones treballadores per no superar el principi de proporcionalitat. Segons l'Audiència Nacional, en aquest cas, tot i que la mesura perseguia una finalitat legítima (el control de l'acompliment de l'activitat laboral), no resultava proporcionada, ja que hauria estat possible implantar un sistema de geolocalització en un dispositiu propietat de l'empresa que no impliqués l'accés a dades personals. En el supòsit analitzat, per poder descarregar l'aplicació utilitzada calia facilitar informació com el número de telèfon o l'adreça de correu electrònic, la qual cosa suposava un tractament injustificat de dades de caràcter personal. A més, el tribunal va assenyalar que la compensació econòmica oferta per l'empresa per "contrarestar" l'obligació d'aportar un dispositiu propi no resultava suficient per entendre superat el principi de proporcionalitat.

Finalment, l'Audiència Nacional sosté, en aquesta mateixa sentència, que exigir unilateralment a les persones treballadores l'aportació d'un dispositiu de la seva propietat i responsabilitzar-les del seu correcte funcionament constitueix un abús de dret empresarial, contrari a la nota d'alienitat que caracteritza les relacions laborals.

Es pot acordar mitjançant pacte amb la persona treballadora que aquesta porti un dispositiu de la seva propietat per instal·lar un sistema de geolocalització?

No es considera lícit que l'empresa obligui unilateralment les persones treballadores a proporcionar un dispositiu de la seva propietat per instal·lar un sistema de geolocalització (Sentència de l'Audiència Nacional núm. 13/2019, de 6 de febrer de 2019, confirmada per la Sentència del Tribunal Suprem núm. 163/2021, de 8 de febrer de 2021).

No obstant això, en principi, sí que hi hauria la possibilitat que s'utilitzés un dispositiu propietat de la persona treballadora per conèixer la seva localització, quan aquesta decisió fos fruit d'un acord entre l'empresa i la persona treballadora i es proporcionés una compensació adequada per això. En aquests supòsits, es requeriria, en tot cas, que el consentiment de la persona treballadora fos vàlid. Tanmateix, en l'àmbit laboral, aquest requisit resulta difícil de complir. El desequilibri existent en la relació contractual sol

impedir que el consentiment sigui veritablement lliure, en existir el temor de patir conseqüències negatives si es nega.

El Tribunal Suprem, en la seva Sentència de 21 de setembre de 2015 (rec. 259/2014) va entendre que el consentiment no podia considerar-se lliure i voluntari quan la clàusula que autoritzava l'empresa, en aquest supòsit, a tractar les dades personals es trobava inclosa en el propi contracte de treball inicial, atès que les persones treballadores podien acceptar aquesta clàusula per por de no ser contractades si expressaven el seu desacord.

És vàlida una clàusula contractual que permet sancionar la persona treballadora per no aportar el seu dispositiu mòbil o descarregar el sistema de geolocalització?

No es pot considerar vàlida una clàusula contractual que contempli la possibilitat de sancionar les persones treballadores per no aportar el seu dispositiu mòbil o per no descarregar l'aplicació que incorpora el sistema de geolocalització. Sobre aquest punt es va pronunciar l'Audiència Nacional en la seva Sentència núm. 13/2019, de 6 de febrer de 2019, posteriorment confirmada per la Sentència del Tribunal Suprem núm. 163/2021, de 8 de febrer de 2021.

En el supòsit enjudiciat per l'Audiència Nacional, l'empresa, a banda d'exigir a les persones treballadores que aportessin els seus propis dispositius mòbils per instal·lar un sistema de geolocalització, va incloure en els contractes de treball una clàusula que preveia sancions disciplinàries en cas d'incompliment d'aquesta obligació. L'Audiència Nacional va declarar nul·la tant la mesura empresarial com la clàusula que establia el règim disciplinari.

Sobre la nul·litat de la clàusula, el tribunal va argumentar que no es pot establir un règim d'infraccions i sancions mitjançant el contracte individual de treball, atès que, conforme a l'article 58.1 de l'Estatut dels Treballadors, aquesta competència correspon a la negociació col·lectiva. Així mateix, va destacar que l'aplicació d'aquest tipus de clàusules resolutòries, que a la pràctica operen com una causa d'acomiadament disciplinari, permetrien l'extinció del contracte sense respectar les garanties formals i de culpabilitat exigides pels articles 54 i 55 de l'ET per als acomiadaments disciplinaris. Per això, en definitiva, no es poden considerar vàlides.

Quant de temps pot conservar l'empresa les dades derivades del sistema de geolocalització?

La normativa sobre protecció de dades no estableix un període màxim de conservació de les dades derivades dels sistemes de geolocalització. No obstant això, com en qualsevol tractament de dades personals, és aplicable el principi de limitació del termini de conservació; per la qual cosa les dades personals obtingudes dels sistemes de geolocalització no podran ser conservades durant més temps del necessari per a les finalitats del tractament (art. 5.1.e) RGPD). Sobre aquest punt, ha de ser assenyalat que el Grup de Treball de l'Article 29 –que era l'òrgan consultiu de la Unió Europea en matèria de protecció de dades, ara substituït pel Comitè Europeu de Protecció de Dades– va recomanar, en el Dictamen 5/2005, que el termini de conservació de les dades de localització relatives a una persona treballadora no fos superior a dos mesos.

Per la seva banda, en el cas específic en què s'emprin les dades de geolocalització per registrar la jornada de les persones treballadores, l'empresa té el deure de conservar els registres durant quatre anys (art. 34.9 ET).

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

Un incompliment de la normativa que regula l'ús de sistemes de geolocalització en el lloc de treball –p. ex., l'ús de sistemes de geolocalització sense haver informat o el seu ús fora de la jornada laboral quan el dispositiu pot ser utilitzat amb finalitats particulars– 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 (art. 183 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 el 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 sistemes de geolocalització, en:

- 12.000 euros, per vulneració del dret a la intimitat i del dret a la llibertat sindical en haver instal·lat un sistema de geolocalització, que seguia en funcionament fora de la jornada de treball, sense complir els deures d'informació (Sentència del Tribunal Superior de Justícia de Madrid núm. 763/2019, de 12 de juliol de 2019).

La vulneració de drets fonamentals també pot tenir lloc en l'obtenció de la prova que és emprada per l'empresa per acreditar un acomiadament d'una persona treballadora. En aquests supòsits, la persona treballadora podrà presentar demanda per acomiadament, al·legant que la prova ha de ser declarada il·lícita en haver mediat vulneració de drets fonamentals (art. 90.2 LRJS). Si no s'admet la prova i l'empresa no pot provar la infracció comesa per la persona treballadora per altres mitjans, l'acomiadament serà declarat improcedent (entre d'altres, Sentència del Tribunal Superior de Justícia de Canàries de Las Palmas de Gran Canària núm. 62/2023, de 18 de gener de 2023; Sentència del Tribunal Superior de Justícia de Castella-la Manxa núm. 487/2015, de 28 d'abril de 2015) o nul (entre d'altres, Sentència del Tribunal Superior de Justícia de Madrid núm. 432/2021, de 14 de juny de 2021; Sentència del Tribunal Superior de Justícia de Catalunya núm. 2713/2025, de 15 de maig de 2025); depenent de si l'òrgan judicial entén que la lesió de drets fonamentals es projecta també sobre la decisió extintiva. En alguns supòsits la declaració de nul·litat o improcedència de l'acomiadament ha anat acompanyada del reconeixement d'una indemnització per danys morals:

- 6.250 euros, per vulneració del dret a la intimitat i del dret a la protecció de dades en haver-se instal·lat un sistema GPS en el vehicle de la persona treballadora que permetia registrar la seva ubicació també fora de la jornada laboral, sense haver-li informat prèviament d'aquesta circumstància (Sentència del Tribunal Superior de Justícia de Madrid núm. 432/2021, de 14 de juny de 2021).
- 6.251 euros, per vulneració del dret a la intimitat en haver-se instal·lat un GPS en l'equip de treball sense el seu coneixement (Sentència del Tribunal Superior de Justícia de Canàries de Las Palmas de Gran Canària núm. 62/2023, de 18 de gener de 2023).
- 7.501 euros, per vulneració del dret a la intimitat i del dret a la protecció de dades en haver-se col·locat un sistema GPS en el vehicle de la persona treballadora sense informació prèvia (Sentència del Tribunal Superior de Justícia de Catalunya núm. 2713/2025, de 15 de maig de 2025).

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 l'ús de sistemes de geolocalització 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'actuació⁴). 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.

⁴ Per a conèixer l'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades, vegeu: <https://apdcat.gencat.cat/es/documentacio/preguntes-freqüents/Ambit-actuacio-Autoritat-Catalana-de-Proteccio-de-Dades/index.html>

- 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.

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, cancel·lació i oposició. Si una empresa s'ha negat a permetre-li a una persona treballadora, per exemple, l'accés a les seves dades de localització, l'autoritat podrà requerir a l'empresa perquè atengui el dret sol·licitat; 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 relatius a l'ús de sistemes de geolocalització 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 de la geolocalització es troben:

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

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

La introducció de sistemes de geolocalització en el lloc de treball pot tenir efectes negatius en la salut de les persones treballadores. El constant monitoratge de la localització de la persona treballadora, la determinació del ritme de treball a través de sistemes de geolocalització, la necessitat d'adaptació a les noves tecnologies o la dificultat de conciliar la vida familiar i laboral són factors de risc psicosocial que poden propiciar l'aparició de patologies com estrès, ansietat o depressió en les persones treballadores⁵.

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.

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 geolocalització.
- L'obligació d'implementar mesures preventives per eliminar o reduir i controlar els riscos manifestats (art. 16.2.b) LPRL).

⁵ Aquests factors de risc psicosocial són esmentats de forma genèrica en el 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.

- 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 GPS.

A més, l'empresa haurà de consultar a les persones delegades de prevenció la introducció dels sistemes de geolocalització 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 GPS 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).

2.3. 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 seua 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 conflueix unes 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 avaluació⁶ 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.

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

- 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.
- 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 de 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 llei⁷.

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 REGAGE25e00024730156⁸, 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

⁷ Vegeu: https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_es.pdf
<https://www.aepd.es/documento/regage25e00024730156.pdf>

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.

2.3.1. 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 biomètrics⁹, 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).

⁹ Vegeu: <https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf>

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.

2.3.2. 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 REGAGE25e00024730156¹⁰. En aquesta consulta es va entendre que era proporcional i comptava amb base legal i 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 avaluació¹¹ 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:

¹⁰ Vegeu: <https://www.aepd.es/documento/regage25e00024730156.pdf>

¹¹ Vegeu: <https://www.aepd.es/documento/listas-dpia-es-35-4.pdf>

- 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.

2.3.3. 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 unes 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 interfereixen 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'eficax); i
- c) ha de ser proporcionada en sentit estricte (que aportí 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'eficax –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.

2.3.4. 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 peril·losos, 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).

2.3.5. 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 empen 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 treballadores¹². 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.

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

¹² En les Directrius de la Comissió sobre les pràctiques d'intel·ligència artificial prohibides que s'estableixen en el Reglament (UE) 2024/1689 (Reglament d'Intel·ligència Artificial), publicades el 29/07/2025. Vegeu: <https://ec.europa.eu/newsroom/dae/redirection/document/118659>

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 demostrï 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 sàpiguin que estan interactuant amb una IA i no amb un ésser humà (art. 50.1 RIA).

2.3.6. 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.

2.3.7. 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'actuació¹³). 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.

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

¹³ Per a conèixer l'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades, vegeu: <https://apdcat.gencat.cat/es/documentacio/preguntes-freqüents/Ambit-actuacio-Autoritat-Catalana-de-Proteccio-de-Dades/index.html>

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 siguin contraris al respecte a la intimitat i consideració deguda a la dignitat de les persones treballadores (art. 8.11 LISOS).

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).

2.4. Davant el registre de l'ordinador i del telèfon mòbil

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

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

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

L'ús de dispositius personals per part de les persones treballadores no es troba expressament regulat en la normativa vigent. No obstant això, encara que l'article 87 de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals no ho esmenti de forma específica, l'empresa ha de, en tot cas, garantir el dret a la intimitat de les persones treballadores quan utilitzin els seus propis dispositius per a fins laborals.

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

De fet, l'Audiència Nacional, en la seva Sentència núm. 13/2019, de 6 de febrer de 2019 (que va ser posteriorment confirmada per la Sentència del Tribunal Suprem núm. 163/2021, de 8 de febrer de 2021) va declarar la nul·litat d'una mesura empresarial que obligava les persones treballadores amb categoria de repartidor/a a aportar un telèfon mòbil de la seva propietat, i a instal·lar-hi una aplicació informàtica de l'empresa que permetia conèixer la geolocalització de la persona treballadora per entendre que no era

proporcionada. Es va considerar que aquesta mesura era contrària al dret a la protecció de dades de les persones treballadores per no superar el principi de proporcionalitat, ja que hauria estat possible implantar un sistema de geolocalització en un dispositiu propietat de l'empresa que no impliqués l'accés a dades personals. En el supòsit analitzat, per poder descarregar l'aplicació utilitzada calia facilitar informació com el número de telèfon o l'adreça de correu electrònic, la qual cosa suposava un tractament injustificat de dades de caràcter personal.

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

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

Els dispositius que són posats a disposició per l'empresa a les persones treballadores no són considerats efectes particulars, de manera que el seu registre no està subjecte a les garanties previstes en l'article 18 de l'Estatut dels Treballadors (assistència d'un/a representant legal o d'una altra persona treballadora, etc.). En tractar-se de dispositius de propietat empresarial, l'empresa podrà realitzar un examen del seu contingut en virtut de les seves potestats de control i direcció (art. 20.3 ET). De fet, la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals preveu expressament la possibilitat que l'empresa pugui accedir al contingut dels dispositius digitals facilitats a les persones treballadores (art. 87 LOPDGDD).

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

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

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

- Només podrà accedir als continguts dels dispositius digitals per controlar el compliment de les obligacions laborals o estatutàries o per garantir la integritat dels dispositius (art. 87.2 LOPDGDD).
- Haurà d'elaborar uns criteris d'utilització dels dispositius digitals amb la participació de la RLPT. Aquests criteris hauran, en tot cas, de respectar els estàndards mínims de protecció de la intimitat de les persones treballadores d'acord amb els usos socials i els drets reconeguts constitucionalment i legalment (art. 87.3 LOPDGDD).
Es tracta d'un deure que té caràcter imperatiu, és a dir, l'empresa té l'obligació d'elaborar els criteris d'ús quan proporcioni a les persones treballadores dispositius digitals per a la realització del treball.
- Haurà d'informar les persones treballadores dels criteris d'utilització elaborats i de la possibilitat de realitzar controls sobre l'ús o contingut del dispositiu digital (art. 87.3 LOPDGDD).

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

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

- Les prohibicions d'ús, absolutes o parcials; és a dir amb quines finalitats pot utilitzar la persona treballadora el dispositiu.
Si es permet l'ús amb finalitats privades, l'empresa haurà d'especificar de manera precisa els usos autoritzats i s'hauran d'establir garanties per preservar la intimitat de les persones treballadores. La normativa posa com a exemple de garantia la determinació dels períodes en què els dispositius podran ser emprats amb finalitats particulars (art. 87.3 LOPDGDD).
- La possibilitat que l'empresa realitzi un registre dels dispositius amb fins de control i les conseqüències disciplinàries que en poguessin derivar.
- Les eines de control que seran emprades per vigilar el compliment de les obligacions laborals.

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

Les persones treballadores hauran de ser informades dels criteris d'utilització que siguin elaborats per l'empresa (art. 87.3 LOPDGDD). Aquesta informació haurà de ser

transmesa amb caràcter previ a l'ús dels dispositius digitals, ja que la persona treballadora ha de ser informada amb antelació de l'abast i la naturalesa de les activitats de monitoratge i de la possibilitat que l'empresa accedeixi al contingut dels dispositius (Sentència del Tribunal Europea de Drets Humans, de 5 de setembre de 2017, Cas Bărbulescu contra Romania). Per això, no serà vàlida la informació simultània a la intervenció o registre (Sentència del Tribunal Superior de Justícia de la Regió de Múrcia, núm. 82/2022, de 26 de gener de 2022).

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

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

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

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

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

Quan l'empresa proporciona a les persones treballadores dispositius digitals per a la realització de la prestació laboral, l'empresa té l'obligació d'elaborar uns criteris

d'utilització d'aquests dispositius (art. 87.2 LOPDGDD). Per això, si accedeix al contingut d'un dispositiu d'una persona treballadora, per corroborar, per exemple, la comissió d'un acte il·lícit, sense haver prèviament complert amb aquesta obligació s'ha d'entendre, en principi, que la prova obtinguda no seria vàlida; en haver-se produït una lesió del dret fonamental a la intimitat. La lesió es produeix perquè la persona treballadora no té coneixement que l'empresa pot accedir al contingut dels dispositius digitals. Si no s'estableix expressament que els dispositius no poden ser emprats amb finalitats privades, la persona treballadora pot entendre que té certa privacitat en l'ús de les eines digitals de treball (p. ex., Sentència del Tribunal Superior de Justícia de Canàries núm. 347/2023, de 21 d'abril de 2023).

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

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

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

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

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

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

Aquest supòsit podria produir-se, per exemple, quan la política empresarial atorgui a l'empresa la facultat d'accedir de forma indiscriminada, continuada i absoluta als

dispositius digitals. De fet, el Tribunal Suprem en la Sentència núm. 225/2024, de 6 de febrer de 2024, tot i no analitzar el contingut dels criteris d'utilització que havia confeccionat l'empresa, assenyala que "tan àmplies possibilitats d'accés poguessin, en el seu cas, col·lidir greument amb els drets a la intimitat i dignitat dels treballadors", qualificant de discutible el contingut dels criteris. La política empresarial sobre l'ús dels dispositius digitals, en aquest cas, establia que: "[...] tots els ordinadors i totes les adreces de correu electrònic corporatius facilitats per l'EMPRESA al TREBALLADOR o utilitzats per aquest en ocasió del seu treball, seran accessibles per l'EMPRESA, podent ser els ordinadors, el seu contingut així com qualsevol arxiu guardat en els mateixos pel TREBALLADOR en qualsevol moment, analitzats, examinats, formatjats i/o restablerts mitjançant els oportuns mitjans informàtics a l'abast de l'empresa (auditoria informàtica, examen pericial informàtic, programari de captura de pantalles, etc.)".

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

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

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

- Quan la política empresarial permet l'ús particular dels dispositius, s'aplica un nivell de protecció de la intimitat de la persona treballadora més reforçat o estricte, principalment perquè s'entén que la persona treballadora emmagatzemarà informació privada i personal en el dispositiu. Per aquesta raó, la normativa estableix que l'empresa haurà d'especificar els usos autoritzats i establir garanties per preservar la intimitat de les persones treballadores (art. 87.3 LOPDGDD). En aquests supòsits, les facultats de control de l'empresa es veuen limitades i només en situacions excepcionals i justificades podria accedir al contingut (p. ex., si s'ha establert expressament que una aplicació no podrà ser utilitzada amb finalitats particulars).
- Quan la política empresarial prohibeix l'ús personal dels dispositius, el nivell de protecció de la intimitat de la persona treballadora disminueix. No obstant això, fins i tot en aquests supòsits, s'entén que la intimitat de les persones treballadores no desapareix. Per això, no quedarà justificada qualsevol mesura de control, sinó

aquelles que responguin a una raó legítima i compleixin amb el principi de proporcionalitat.

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

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

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

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

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

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

emoticones i la persona acomiadada ni la possible imputació d'assetjament laboral.

- *Principi de proporcionalitat.* La mesura de control haurà de superar a més el principi de proporcionalitat:

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

En termes generals, el principi de proporcionalitat exigeix demostrar que la finalitat no podia ser assolida amb altres mètodes menys intrusius i que el registre es va limitar a l'estrictament necessari i no es va realitzar de forma indiscriminada. Un supòsit en el qual es va considerar proporcionat l'accés al compte de correu electrònic corporatiu de la persona treballadora és el descrit en la Sentència del Tribunal Suprem núm. 119/2018, de 8 de febrer de 2018. La recerca es va limitar a l'objectiu de trobar correus relacionats amb les transferències bancàries trobades a la fotocopidora; emprant-se paraules claus i acotant el registre a les dates pròximes a les transferències.

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

- Es va gravar la pantalla de l'ordinador de la persona treballadora durant tres dies per comprovar si treballava durant la seva jornada. Es va considerar que aquest monitoratge era excessiu perquè permetia fins i tot visualitzar correus personals i a més ja hi havia testimonis (altres persones treballadores) que podien demostrar que la persona no estava treballant la major part del temps (Sentència del Tribunal Superior de Justícia de Madrid núm. 591/2018, de 13 de setembre de 2018).
- Es va instal·lar un programa informàtic en tots els ordinadors propietat de l'empresa per monitorar el seu ús i comprovar si les persones treballadores empraven l'ordinador amb finalitats particulars. Es va acomiadar una persona treballadora perquè accedia a pàgines web alienes a l'àmbit professional. Es va entendre que no era proporcionada la mesura perquè l'objectiu podia aconseguir-se amb mètodes menys intrusius com la restricció de l'accés a certes pàgines web o la supervisió del trànsit en internet o de l'ús de la missatgeria electrònica, però sense examinar el seu contingut (Sentència del Tribunal Superior de Justícia de la Comunitat Valenciana núm. 3390/2018, de 19 de novembre de 2018).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

genèric susceptible de determinació individual, els sindicats que tinguin un àmbit d'actuació igual o major al del conflicte també podran iniciar un procediment judicial.

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

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

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

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

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

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

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

Finalment, cal esmentar que l'Agència Espanyola de Protecció de Dades no té competència per garantir el compliment ni l'exercici de les garanties establertes a l'article 87 LOPDGDD, tal com es recull a la Resolució E/10250/2019, de 3 de juny de 2020¹⁴.

¹⁴ Vegeu: <https://www.aepd.es/documento/e-10250-2019.pdf>

2.5. Davant el registre de jornada

Quins requisits ha de complir un sistema de registre de jornada?

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).

L'Estatut dels Treballadors no estableix una forma concreta en la qual s'hagi d'efectuar el registre de jornada, sinó que deixa a la negociació col·lectiva, a l'acord d'empresa o a la decisió empresarial, prèvia consulta amb la RLPT, la possibilitat de concretar el sistema de registre, la seva organització i documentació.

Aquesta absència de concreció de l'article 34.9 de l'Estatut dels Treballadors sobre la forma en què s'ha de materialitzar el control horari ha estat completada per la jurisprudència del Tribunal de Justícia de la Unió Europea, qui en la seva Sentència de 14 de maig de 2019 (assumpte C-55/18) va argumentar que un sistema de registre horari havia de proporcionar, en tot cas, informació objectiva, fiable i accessible.

Per la seva banda, el Ministeri de Treball, Migracions i Seguretat Social va elaborar en 2019 una Guia sobre el registre de jornada, en la qual va disposar que serà vàlid qualsevol sistema o mitjà, en suport paper o telemàtic que proporcioni informació fiable, immodificable i no manipulable a posteriori. Tot i que cal esmentar que els sistemes de registre en paper poden no ser adequats per al compliment de l'obligació legal. L'Audiència Nacional, en la seva Sentència núm. 22/2022, de 15 de febrer de 2022, va concloure que un sistema de registre basat en la signatura en un full de paper no era un mitjà vàlid per complir amb el deure de control horari, ja que dificultava la posada a disposició de la informació a les persones interessades i no garantia la fiabilitat de la informació. A més, en aquest supòsit l'hora d'inici de la jornada estava predeterminada i l'hora de finalització es calculava de forma estimada.

Finalment, cal afegir que l'obligació de registre s'estén també sobre les hores extraordinàries (art. 35.5 ET) i sobre la jornada de les persones treballadores a temps parcial (art. 12.4 ET) i a distància (art. 14 LTD).

Quins mitjans de registre poden ser emprats?

Aplicant la normativa laboral, per complir l'obligació legal de registre horari podrà ser emprat, en principi, qualsevol mitjà que permeti recaptar la informació relativa a la jornada diària de les persones treballadores, de forma accessible, objectiva i fiable.

Ara bé, abans d'implementar qualsevol sistema de registre, l'empresa ha de tenir en consideració que es pot veure afectat el dret a la intimitat i/o el dret a la protecció de dades de les persones treballadores, en la mesura que aquests sistemes impliquen el tractament de dades personals.

Els sistemes de registre de jornada han d'incloure informació sobre l'horari concret d'inici i finalització de la jornada de cada persona treballadora. Per garantir un adequat compliment d'aquesta obligació, el sistema de registre ha de contenir informació personal, ja que cal vincular les dades registrades relatives a l'horari amb la persona treballadora que correspongui. A més, hi ha sistemes que poden ser més intrusius en recaptar dades especialment sensibles com les dades biomètriques (sistemes de reconeixement facial o d'escàner de l'empremta dactilar).

En conseqüència, en instal·lar un sistema de registre horari, l'empresa haurà de complir la normativa en matèria de protecció de dades, garantint el respecte als principis i obligacions establerts pel Reglament General de Protecció de Dades i per la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

Quan s'instal·la un sistema de registre de jornada, quina és la base jurídica del tractament de les dades personals?

Quan s'instal·la un sistema de registre de jornada, el tractament de les dades personals ve justificat per l'aplicació de la base legitimadora de l'article 6.1.c) del Reglament General de Protecció de Dades. Es tracta d'un precepte que disposa que el tractament serà lícit quan sigui: "necessari per complir una obligació legal aplicable al responsable del tractament". La base jurídica serà, per tant, l'obligació de registrar la jornada diària de l'article 34.9 de l'ET.

No obstant això, si s'empren sistemes de control horari que tracten dades especialment sensibles, com succeeix amb els sistemes de reconeixement facial o d'escàner d'empremta dactilar basats en dades biomètriques, l'empresa haurà d'acreditar, a més, que concorre una de les circumstàncies recollides a l'article 9.2 del Reglament General de Protecció de Dades, que permeten aixecar la prohibició de tractament que versa sobre aquesta tipologia de dades.

Quins principis ha de complir l'empresa en el tractament de les dades personals?

Com que els sistemes de registre horari contenen informació que permet identificar les persones treballadores, la seva instal·lació comporta un tractament de dades personals.

Aquesta circumstància implica que l'empresa haurà de complir amb la normativa en matèria de protecció de dades i, per tant, amb els principis relatius al tractament de l'article 5 del Reglament General de Protecció de Dades (RGPD).

En relació amb el registre de jornada, l'Agència Espanyola de Protecció de Dades, a la Guia sobre la protecció de dades en les relacions laborals, emfatitza la importància d'observar els principis de minimització de dades (art. 5.1.c) RGPD) i limitació de la finalitat (art. 5.1.b) RGPD). D'una banda, el principi de minimització de dades exigeix que el registre de jornada només emmagatzemi aquelles dades personals que siguin imprescindibles. I, d'altra banda, el principi de limitació de la finalitat implica que no podran ser utilitzades les dades del registre amb una finalitat diferent del control horari. Per tant, en el supòsit en què, per exemple, s'instal·lés un sistema de registre que captés la ubicació de la persona treballadora, l'empresa no podria usar el GPS per conèixer la localització continuada de la persona, sinó només per controlar el temps de treball. A més, si la intenció de l'empresa és emprar el sistema de registre de jornada per supervisar l'activitat laboral i aplicar mesures disciplinàries més enllà del control del temps de treball, haurà d'informar d'aquesta finalitat les persones treballadores des d'un inici, havent de justificar igualment la legitimitat de la mesura de control.

A més dels principis relatius al tractament, el sistema de registre que s'implementi haurà de superar el principi de proporcionalitat, en tractar-se d'una mesura que pot lesionar drets fonamentals (concretament el dret a la intimitat i el dret a la protecció de dades). Per comprovar que el sistema és adequat, s'ha de constatar que compleix tres condicions:

- ha de ser idoni, és a dir, susceptible d'aconseguir l'objectiu proposat;
- ha de ser necessari, és a dir, que no existeixi una altra mesura més moderada per a la consecució d'aquest objectiu i igual d'eficaç; i
- ha de ser proporcionat en sentit estricte, és a dir, que aportï més beneficis per a l'interès general que perjudicis sobre altres béns o valors en conflicte.

Un sistema de registre que podria concloure's que no supera el principi de proporcionalitat és l'ús de microxips intramusculars. Es tracta d'un mitjà excessivament invasiu que podria ser substituït per altres alternatives més moderades.

Quines obligacions ha de complir l'empresa en matèria de protecció de dades?

En primer lloc, l'empresa haurà de complir amb el deure d'informació recollit en el Reglament General de Protecció de Dades (RGPD). L'empresa haurà d'informar les persones treballadores sobre les finalitats per a les quals seran utilitzades les dades

personals (control horari); les persones destinatàries de la informació; el termini durant el qual es conservaran les dades personals; 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). A més, 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).

En segon lloc, l'empresa haurà d'implementar mesures de seguretat per garantir la confidencialitat de les dades del registre (art. 32 RGPD). D'aquesta manera, l'empresa haurà d'assegurar que no puguin accedir a la informació del registre de jornada persones no autoritzades per llei (sí que estarien autoritzades les persones treballadores interessades, la RLPT i la ITSS).

En tercer lloc, l'empresa haurà d'elaborar una avaluació d'impacte relativa a la protecció de dades en aquells supòsits en què el sistema de registre pugui implicar un alt risc per als drets i llibertats de les persones (art. 35 RGPD). L'Agència Espanyola de Protecció de Dades, a la Guia sobre la protecció de dades en les relacions laborals, disposa que, quan s'instal·la un sistema de registre, l'avaluació d'impacte relativa a la protecció de dades pot ser necessària depenent del nombre de persones treballadores de l'empresa i del format emprat. Per exemple, la implementació d'un sistema de control biomètric requerirà, en tot cas, la realització de l'avaluació d'impacte perquè utilitza dades especialment sensibles.

En definitiva, quan el sistema pugui implicar un alt risc, l'empresa 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.

Pot l'empresa emprar tecnologies de biometria per registrar la jornada?

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 Tribunal de Justícia de la Unió Europea (Sentència de 14 de maig de 2019 (assumpte C-55/18)) que, en tot cas, haurà de tractar-se d'un sistema que proporcioni informació objectiva, fiable i accessible.

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 biomètrics¹⁵, 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.

¹⁵ Vegeu: <https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf>

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 utilitzat fins al moment i les raons per les quals ja no són adequats aquests sistemes.

Aquesta anàlisi de la necessitat del sistema biomètric hauria de quedar igualment plasmada en l'avaluació d'impacte relativa a la protecció de dades. En emprar dades especialment sensibles, un sistema de control biomètric pot suposar un alt risc per als drets i llibertats de les persones; per això, l'empresa té l'obligació de realitzar una avaluació d'impacte abans d'iniciar el tractament de dades biomètriques (art. 35 RGPD). L'avaluació d'impacte relativa a la protecció de dades, en tot cas, ha d'incloure: una descripció sistemàtica de les operacions del tractament i dels fins; una avaluació de la necessitat i proporcionalitat del sistema; una avaluació dels riscos per als drets i llibertats de les persones treballadores; i una descripció de les mesures previstes per afrontar aquests riscos.

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).

Pot l'empresa implementar un sistema de geolocalització per registrar la jornada?

Els sistemes de geolocalització podrien ser un mitjà vàlid per al compliment de l'obligació de control horari. No obstant això, en produir-se un tractament de dades personals i veure's afectats els drets fonamentals a la intimitat i a la protecció de dades, en la seva

utilització s'haurà d'observar el principi de proporcionalitat, i els principis de minimització i limitació de la finalitat recollits en el Reglament General de Protecció de Dades:

- D'una banda, el principi de proporcionalitat implica que només podrà emprar-se un sistema de geolocalització per registrar la jornada quan sigui realment necessari per les característiques de l'activitat laboral: per exemple, en supòsits en què el treball es realitza fora de les dependències de l'empresa i presti serveis localitzats (Sentència del Tribunal Superior de Justícia d'Andalusia núm. 1662/2023, de 21 de setembre de 2023).
- D'altra banda, segons el que disposa l'Agència Espanyola de Protecció de Dades, en la Guia sobre la protecció de dades en les relacions laborals, els principis de minimització i limitació de la finalitat suposen que el tractament de les dades de geolocalització haurà de quedar reclus al compliment de l'obligació legal de registre. En altres paraules, es podrà comprovar la ubicació de la persona treballadora exclusivament en aquells moments en què s'iniciï o finalitzi la jornada laboral; quedant injustificat l'accés a les dades de geolocalització durant la totalitat de la durada d'aquesta.

A més, s'haurà de complir el que disposa l'article 90 de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, havent d'informar les persones treballadores i la RLPT sobre l'existència i característiques del sistema de geolocalització. No obstant això, en alguns supòsits, els tribunals han considerat que no existia vulneració del dret a la intimitat i/o del dret a la protecció de dades quan, tot i que l'empresa no havia facilitat la informació exigida de forma individualitzada i expressa, la utilització de sistemes de geolocalització estava prevista en el conveni col·lectiu aplicable (Sentència del Tribunal Superior de Justícia d'Andalusia núm. 1662/2023, de 21 de setembre de 2023).

Pot l'empresa establir un sistema de videovigilància per controlar l'horari de treball?

Els sistemes de videovigilància podrien ser un mitjà vàlid per al compliment de l'obligació de control horari. No obstant això, en produir-se un tractament de dades personals i veure's afectats els drets fonamentals a la intimitat i a la protecció de dades, en la seva utilització s'haurà d'observar el principi de proporcionalitat, i els principis de minimització i limitació de la finalitat recollits en el Reglament General de Protecció de Dades:

- D'una banda, el principi de proporcionalitat implica que solament podrà emprar-se un sistema de videovigilància per registrar la jornada quan sigui realment necessari per les característiques de l'activitat laboral.
- D'altra banda, els principis de minimització i limitació de la finalitat suposen que l'ús de les imatges haurà de quedar reclòs al compliment de l'obligació legal de registre. En altres paraules, es podrà captar la imatge de la persona treballadora per comprovar l'horari de la persona treballadora; quedant injustificat l'accés a les imatges durant la totalitat de la durada de la jornada i per a altres fins aliens a aquest control.

Finalment, en tot cas, s'haurà de complir el que disposa l'article 89 de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, havent d'informar les persones treballadores i la RLPT sobre l'existència del sistema de videovigilància i no podent instal·lar càmeres que enfoquin a llocs destinats al descans o esbargiment.

Pot l'empresa emprar un sistema de gravació de veu per registrar la jornada?

La Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, en l'article 89, prohibeix l'ús de sistemes de gravació de sons en el lloc de treball, llevat quan siguin necessaris per garantir la seguretat de les instal·lacions, béns i persones que es trobin en el centre de treball i, en tot cas, respectin el principi de proporcionalitat (és a dir, superin els principis d'idoneïtat, necessitat i proporcionalitat en sentit estricte). Per això, amb caràcter general, no es podran utilitzar sistemes de gravació de veu per registrar la jornada de treball de les persones treballadores. En principi, hi ha altres mitjans menys intrusius que poden complir amb l'obligació de registre horari, per la qual cosa difícilment es pot considerar que superen el principi de proporcionalitat.

A més, la veu és una dada biomètrica, per la qual cosa s'hauria d'acreditar la superació de la prohibició de tractament que recau sobre el tractament de dades especialment sensibles (art. 9.2 RGPD).

Es pot establir un sistema de registre en paper?

L'empresa té el deure d'implantar un sistema de registre que proporcioni informació objectiva, fiable i accessible sobre l'horari concret d'inici i fi de la jornada diària de cada persona treballadora (Sentència del Tribunal de Justícia de la Unió Europea de 14 de maig de 2019 (assumpte C-55/18) i art. 34.9 ET). A més, ha de garantir que aquesta informació pugui ser posada a disposició de les persones treballadores, la RLPT i la ITSS.

Si bé la normativa sobre registre horari no estableix una forma concreta en la qual s'hagi d'efectuar el registre, les exigències que neixen de l'article 34.9 de l'ET i de la jurisprudència del Tribunal de Justícia de la Unió Europea, dificulten que un sistema de registre en paper pugui entendre's adequat per complir amb l'obligació legal. A més de posar en dubte la fiabilitat de la informació que conté, un sistema basat en la signatura en un full de paper pot dificultar la posada a disposició de la informació a les parts interessades (Sentència de l'Audiència Nacional núm. 22/2022, de 15 de febrer de 2022).

Es pot obligar la persona treballadora a aportar un dispositiu de la seva propietat per registrar la jornada?

L'empresa no pot obligar unilateralment la persona treballadora a aportar un dispositiu digital de la seva propietat per complir amb l'obligació legal de registrar la jornada, és a dir, per accedir a través d'aquests a les aplicacions o programes corporatius que permetin controlar l'horari de la persona treballadora.

Aquesta exigència constitueix un abús de dret empresarial, contrari a la nota d'alienitat que caracteritza les relacions laborals. Es tracta d'una conclusió que va ser obtinguda per l'Audiència Nacional, en la seva Sentència núm. 13/2019, de 6 de febrer de 2019 (posteriorment confirmada per la Sentència del Tribunal Suprem núm. 163/2021, de 8 de febrer de 2021), en la qual va declarar la nul·litat d'una mesura empresarial que obligava a les persones treballadores amb categoria de repartidor/a a aportar un telèfon mòbil de la seva propietat i a instal·lar-hi una aplicació informàtica de l'empresa que permetia conèixer la geolocalització de la persona treballadora.

Per això, l'empresa haurà de recaptar el consentiment de la persona treballadora si requereix que aquesta empli el seu dispositiu personal per complir amb l'obligació legal de registre de jornada. Un consentiment que ha de ser vàlid i prestat lliurement, sense que existeixi el temor de patir conseqüències negatives si es nega.

El Tribunal Suprem, en la seva Sentència de 21 de setembre de 2015 (rec. 259/2014) va entendre que el consentiment no podia considerar-se lliure i voluntari quan la clàusula que autoritzava l'empresa, en aquest supòsit, a tractar les dades personals es trobava inclosa en el propi contracte de treball inicial, atès que les persones treballadores podien acceptar aquesta clàusula per por de no ser contractades si expressaven el seu desacord.

Pot estar col·locat el sistema de registre en un lloc visible i accessible al públic?

La informació relativa al registre de jornada conté dades personals. Per això, el sistema no pot estar localitzat en un lloc d'accés públic o visible per a persones no autoritzades.

Pot la persona treballadora accedir a les dades del registre?

L'Estatut dels Treballadors estableix que els registres romandran a disposició de les persones treballadores (art. 34.9 ET), per la qual cosa l'empresa haurà de garantir a les persones treballadores l'accés a la informació relativa al seu registre de jornada.

El Ministeri de Treball, Migracions i Seguretat Social, en la Guia sobre el registre de jornada, va indicar que aquesta obligació establerta en la normativa havia de ser interpretada en el sentit que sigui possible accedir als registres en qualsevol moment en què siguin sol·licitats per les persones treballadores, entenent que els registres han de romandre físicament en el lloc de treball o ser accessibles des del mateix de forma immediata.

No obstant això, el criteri elaborat pel Ministeri de Treball, Migracions i Seguretat no és vinculant, i els tribunals han entès que l'obligació legal de mantenir el registre horari a disposició de les persones interessades no comporta, per si mateixa, un accés immediat a la informació, llevat que aquesta immediata hagi estat expressament acordada entre la RLPT i l'empresa (Sentència del Tribunal Superior de Justícia de Galícia núm. 4384/2021, d'11 de novembre de 2021; Sentència de l'Audiència Nacional núm. 168/2024, de 9 de desembre de 2024; Sentència de l'Audiència Nacional núm. 28/2025, de 24 de febrer de 2025).

D'altra banda, segons el Ministeri de Treball, Migracions i Seguretat Social, aquesta possibilitat d'accés i consulta de la informació (llevat que així hagi estat acordat entre la RLPT i l'empresa) no implica l'obligació de lliurament de còpies del registre, a diferència del que es succeeix amb les persones treballadores a temps parcial i el registre de les hores extraordinàries. En aquests supòsits, l'Estatut dels Treballadors sí que concreta que l'empresa haurà de lliurar còpia a la persona treballadora, juntament amb el rebut de salaris, del resum mensual de totes les hores realitzades (arts. 12.4 i 35.5 ET).

Pot la ITSS accedir a la informació?

L'Estatut dels Treballadors disposa que els registres romandran a disposició de la Inspecció de Treball i Seguretat Social (art. 34.9 ET).

El Ministeri de Treball, Migracions i Seguretat Social, a la Guia sobre el registre de jornada, va indicar que aquesta obligació establerta en la normativa havia de ser

interpretada en el sentit que sigui possible accedir als registres en qualsevol moment en què siguin sol·licitats per la Inspecció de Treball i Seguretat Social.

Quant de temps ha de conservar les dades del registre?

L'empresa té l'obligació de conservar la informació corresponent als registres durant quatre anys (art. 34.9 ET).

L'Estatut dels Treballadors no es pronuncia sobre el mode de conservació de la informació. No obstant això, aplicant el Criteri Tècnic 101/2019 de la ITSS seria vàlid qualsevol sistema que garanteixi la fiabilitat, veracitat i accessibilitat de les dades registrades diàriament.

Sobre el registre de la jornada de les persones treballadores a temps parcial, l'Estatut dels Treballadors concreta que l'empresa haurà de conservar durant quatre anys els resums mensuals dels registres de jornada (art. 12.4 ET).

Quines conseqüències pot tenir un incompliment de la normativa aplicable sobre registre de jornada?

Un incompliment de la normativa sobre protecció de dades aplicada al registre horari –p. ex., l'ús de sistemes de biometria sense aixecar la prohibició– 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 (art. 183 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 el 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 el registre horari, 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 fixar 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.

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 registre de jornada, 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'actuació¹⁶). 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.

¹⁶ Per a conèixer l'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades, vegeu: <https://apdcat.gencat.cat/es/documentacio/preguntes-freqüents/Ambit-actuacio-Autoritat-Catalana-de-Proteccio-de-Dades/index.html>

- 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.

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, cancel·lació i oposició. Si una empresa s'ha negat a permetre-li a una persona treballadora, per exemple, l'accés a les dades del registre de jornada, l'autoritat podrà requerir a l'empresa perquè atengui el dret sol·licitat; 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 sobre registre horari, 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 registre de jornada es troba:

- La transgressió de les normes i els límits legals o pactats en matèria de jornada, treball nocturn, hores extraordinàries, hores complementàries, descansos, vacances, permisos, registre de jornada i, en general, el temps de treball a què es refereixen els articles 12, 23 i 34 a 38 de l'Estatut dels Treballadors (art. 7.5 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).

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

2.6. 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 empen 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 mostri 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 mateixes 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'indole laboral o la promoció o rescissió de relacions contractuals d'indole 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 d'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 siguin contraris al respecte a la intimitat i consideració deguda a la dignitat de les persones treballadores (art. 8.11 LLISOS).
 - 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'actuació¹⁷). 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).

¹⁷ Per a conèixer l'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades, vegeu: <https://apdcat.gencat.cat/es/documentacio/preguntes-frequents/Ambit-actuacio-Autoritat-Catalana-de-Proteccio-de-Dades/index.html>

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

- La falta d'adopció de mesures 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.

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 depressió¹⁸. 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

¹⁸ 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.

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.

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).

2.7. Davant les EPIs intel·ligents

Què és un EPI intel·ligent?

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

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

La implantació en el lloc de treball d'aquest tipus d'EPIs, si bé pot augmentar la protecció de la persona treballadora, planteja també importants implicacions jurídiques. El seu ús haurà de complir, per tant, amb la normativa vigent, tant europea (Reglament (UE) 2016/425, relatiu als equips de protecció individual; Reglament General de Protecció de Dades; Reglament d'Intel·ligència Artificial, etc.) com a nacional (Llei de Prevenció de Riscos Laboral; Reial Decret 773/1997, sobre disposicions mínimes de seguretat i salut relatives a la utilització pels treballadors d'equips de protecció individual, etc.).

Quan podrien implementar-se EPIs intel·ligents?

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

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

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

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

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

- Tractin categories especials de dades, com les dades de salut o les dades biomètriques dirigides a identificar una persona. L'empresa només podrà utilitzar aquesta tipologia de dades quan acrediti el compliment d'una de les excepcions previstes a l'article 9.2 del RGPD (p. ex., consentiment explícit de la persona treballadora, compliment d'una obligació de Dret laboral, finalitats de medicina preventiva o laboral, etc.).
- Emprin IA i se serveixin de tècniques subliminars, manipuladores o enganyoses amb l'objectiu o l'efecte d'alterar de manera substancial el comportament d'una persona o col·lectiu, minvant de manera apreciable la seva capacitat per prendre una decisió informada i fent que prengui una decisió que provoqui o sigui raonable que provoqui perjudicis considerables a aquesta o altres persones (art. 5.1.a) RIA).
- Utilitzin IA i reconeguin emocions. El Reglament d'Intel·ligència Artificial prohibeix que els sistemes d'IA se serveixin de dades biomètriques, com, p. ex., el rostre o la veu, per distingir o inferir les emocions o les intencions de les persones treballadores; excepte quan la seva implementació respongui a motius mèdics o de seguretat (art. 5.1.f) RIA). L'aplicació en el lloc de treball d'EPIs que integrin sistemes de reconeixement d'emocions podria emmarcar-se en l'excepció prevista pel RIA. No obstant això, en aquests supòsits, s'hauria d'identificar expressament per què és necessària l'aplicació d'aquesta tipologia de sistemes per

a la prevenció de riscos laborals i acreditar-se per què no existeix una altra alternativa menys intrusiva que pogués complir amb la mateixa finalitat.

La Comissió Europea ha assenyalat¹⁹ que l'excepció de motius mèdics o de seguretat ha de ser interpretada restrictivament i que no empara, per tant, la implementació de sistemes de reconeixement d'emocions per controlar el benestar general de les persones treballadores (si pateixen estrès, ansietat, si estan avorrides, etc.) quan no existeix un perill específic que requereixi el monitoratge d'aquest. En aquest sentit, la Comissió ha entès que sí que podria existir un risc si, per exemple, s'empren màquines perilloses i un elevat nivell d'estrès pogués posar en perill la salut de les persones treballadores. En aquests excepcionals supòsits, l'empresa no podria utilitzar les dades amb finalitats diferents, com l'avaluació del rendiment de la persona treballadora.

En tot cas, el concepte "emocions" inclou només aspectes com la felicitat, la tristesa o la indignació, deixant fora els estats físics, com el dolor o el cansament. Per la qual cosa, els EPIs sí que podrien integrar IA que dedueixi estats físics.

- Emprin IA i recopilen dades biomètriques, p. ex., el rostre o la veu, per deduir o classificar informació sensible de les persones, com la seva raça, religió, orientació sexual, opinions polítiques o afiliació sindical (art. 5.1.g) RIA). Les empreses no poden utilitzar en el lloc de treball EPIs que intentin "endevinar" aquestes característiques i classificar les persones treballadores d'acord amb elles.

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

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

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

Més concretament, el Reial decret 773/1997, sobre disposicions mínimes de seguretat i salut relatives a la utilització pels treballadors d'equips de protecció individual disposa

¹⁹ En les Directrius de la Comissió sobre les pràctiques d'intel·ligència artificial prohibides que s'estableixen en el Reglament (UE) 2024/1689 (Reglament d'Intel·ligència Artificial), publicades el 29/07/2025. Vegeu: <https://ec.europa.eu/newsroom/dae/redirection/document/118659>

que l'empresa haurà d'informar les persones treballadores, prèviament a l'ús dels EPIs, dels riscos contra els quals els protegeixen i de les activitats o ocasions en les quals s'han d'utilitzar; una informació que haurà de ser transmesa en un format que sigui comprensible per a les persones treballadores. A més, l'empresa haurà de proporcionar-los instruccions, preferentment per escrit, sobre la forma correcta d'utilitzar-los i mantenir-los (art. 8.2).

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

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

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

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

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

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

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

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

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

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

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

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

- Determinar els llocs de treball en què les persones treballadores han de fer ús dels EPIs, així com els riscos davant els quals s'ha d'oferir la protecció, les parts del cos que cal protegir i el tipus d'EPI que s'ha d'utilitzar.
- Elegir els EPIs, atenent les condicions del lloc de treball i de la persona treballadora.
- Proporcionar gratuïtament els EPIs a les persones treballadores.

- Vetllar per una adequada utilització i manteniment dels EPIs (que s'efectuïn d'acord amb les instruccions de l'empresa fabricant).

Quines condicions han de reunir els EPIs intel·ligents?

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

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

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

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

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

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

Els EPIs intel·ligents poden causar accidents o lesions derivats d'un mal funcionament, d'errors en el sistema, de la generació d'informació incorrecta, de la manca d'adaptació de l'equip a les persones treballadores, o de l'excessiva confiança que les persones hi disposen i que pot provocar que no se supervisin les seves indicacions o no es compleixin la resta de les mesures de prevenció. A més, el constant monitoratge de la persona treballadora, l'excés d'informació, la sobrecàrrega cognitiva o la falta de formació tècnica

per poder utilitzar els EPIs intel·ligents són factors de risc psicosocial que poden propiciar l'aparició de patologies com estrès, ansietat o depressió.

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

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

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

- Infraccions greus amb què poden ser sancionades amb multa, en el seu grau mínim, de 2.451 a 9.830 euros; en el seu grau mitjà, de 9.831 a 24.585 euros; i en el seu grau màxim, de 24.586 a 49.180 euros (art. 40.2.b) LISOS):
 - No dur a terme les avaluacions de riscos i, si s'escau, les seves actualitzacions i revisions, així com els controls periòdics de les condicions de treball i de l'activitat de les persones treballadores que escaiguin, o no realitzar aquelles activitats de prevenció que facin necessaris els resultats de les avaluacions, amb l'abast i contingut establerts en la normativa sobre prevenció de riscos laborals (art. 12.1.b) LISOS).
 - Incomplir l'obligació d'efectuar la planificació de l'activitat preventiva que derivi com a necessària de l'avaluació de riscos, o no fer el seguiment d'aquesta, amb l'abast i el contingut establerts en la normativa de prevenció de riscos laborals (art. 12.6 LISOS).
 - L'incompliment de les obligacions en matèria de formació i informació suficient i adequada a les persones treballadores sobre els riscos del lloc de treball susceptibles de provocar danys per a la seguretat i salut i sobre les mesures preventives aplicables, llevat que es tracti d'infracció molt greu conforme a l'article següent (art. 12.8 LISOS).
 - L'incompliment dels drets d'informació, consulta i participació de les persones treballadores reconeguts en la normativa sobre prevenció de riscos laborals (art. 12.11 LISOS).
 - L'incompliment de la normativa de prevenció de riscos laborals, sempre que aquest incompliment creï un risc greu per a la integritat física o la salut

de les persones treballadores afectades i especialment en matèria de: disseny, elecció, instal·lació, disposició, utilització i manteniment dels llocs de treball, eines, maquinària i equips (art. 12.16.b) LISOS).

- No facilitar a les persones treballadores designades o al servei de prevenció l'accés a la informació i la documentació assenyalades en l'apartat 1 de l'article 18 i en l'apartat 1 de l'article 23 de la Llei de Prevenció de Riscos Laborals (art. 12.19 LISOS).

A més, una conducta empresarial que posi en risc la salut de les persones treballadores pot suposar una vulneració del dret a la integritat física i moral (art. 15 CE). En aquests supòsits, les persones treballadores podran presentar demanda de tutela de drets fonamentals expressant els fets que han constituït la vulneració, el dret infringit i la quantia de la indemnització pretesa (art. 183 LRJS).

Si els EPIs recopilen dades personals de les persones treballadores, quines obligacions haurà de complir l'empresa?

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

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

Per això, l'empresa haurà d'elaborar, amb caràcter previ a la instal·lació d'EPIs amb IA integrada o recopilació de dades, una avaluació d'impacte relativa a la protecció de dades que haurà d'incloure, entre altres aspectes: una avaluació de la

necessitat i proporcionalitat de la mesura i dels riscos que tenen sobre els drets de les persones treballadores i una descripció les mesures previstes per afrontar-los (art. 35.7 RGPD).

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

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

Així, la Llei de Prevenció de Riscos Laborals reconeix que l'empresa garantirà a les persones treballadores al seu servei la vigilància periòdica del seu estat de salut en funció dels riscos inherents al treball (art. 22 LPRL). Aquesta vigilància requereix el consentiment de la persona 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 aquest, per a les altres persones treballadores o per a altres persones relacionades amb l'empresa o
- quan així estigui establert en una disposició legal en relació amb la protecció de riscos específics i activitats d'especial perillositat.

En certes situacions, la implementació d'EPIs que recopilen dades de salut de les persones treballadores (freqüència cardíaca, pressió arterial, temperatura corporal, etc.) podria venir justificada per la necessitat de verificar si l'estat de salut de la persona treballadora pot constituir un perill per a la mateixa o altres persones. Tanmateix, la norma exigeix que s'apliquin proves proporcionals al risc, que causin les menors molèsties a la persona treballadora i que es respecti el dret a la intimitat i a la dignitat de la persona. Per això, fins i tot en aquests supòsits excepcionals, s'hauria d'acreditar que el monitoratge de l'estat de salut és una mesura proporcional i imprescindible per al compliment d'un fi, que no pot ser assolit per altres mitjans menys invasius. A més, en tot cas, l'empresa hauria de limitar la recopilació de les dades de salut a aquelles que siguin estrictament necessàries per al compliment de les obligacions de prevenció de riscos laborals.

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

En matèria de protecció de dades, davant un incompliment del Reglament General de Protecció de Dades, es podrà presentar reclamació davant l'Agència Espanyola de Protecció de Dades o davant l'Autoritat Catalana de Protecció de Dades (quan els fets denunciats s'atribueixen a una persona o entitat inclosa dins del seu àmbit d'actuació²⁰). 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):

²⁰ Per a conèixer l'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades, vegeu: <https://apdcat.gencat.cat/es/documentacio/preguntes-freqüents/Ambit-actuacio-Autoritat-Catalana-de-Proteccio-de-Dades/index.html>

- 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.

A més, una conducta empresarial que suposi una intromissió il·legítima en l'esfera privada de les persones treballadores pot suposar una vulneració del dret a la intimitat i/o del dret a la protecció de dades (arts. 18.1 i 18.4 CE). En aquests supòsits, les persones treballadores podran presentar demanda de tutela de drets fonamentals expressant els fets que han constituït la vulneració, el dret infringit i la quantia de la indemnització pretesa (art. 183 LRJS).

3. 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).

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

Quan una empresa lliura dispositius digitals a les persones treballadores per al desenvolupament de la seva activitat laboral, ha d'elaborar els criteris d'utilització d'aquests dispositius, en els quals s'indiqui, entre altres qüestions, les prohibicions d'ús, la possibilitat de realitzar registres i les eines de control que seran emprades per vigilar el compliment de les obligacions laborals (art. 87 LOPDGDD, Sentència del Tribunal

Suprem de 26 de setembre de 2007, rec. 966/2006 i Sentència del Tribunal Europeu de Drets Humans, de 5 de setembre de 2017, Cas Bărbulescu contra Romania).

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

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

L'Audiència Nacional, en la sentència confirmada pel Tribunal Suprem, també recalca que la participació exigida en la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals és equivalent a la consulta recollida en l'article 64 de l'Estatut dels Treballadors, apartats 5 i 6. Per això, la RLPT tindrà dret a emetre un informe previ sobre la qüestió i a reunir-se amb l'empresa per contrastar opinions i poder arribar a un possible acord sobre el contingut dels criteris d'utilització.

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

Té dret la RLPT a accedir a la informació del registre de jornada?

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) i el deure de garantir que els registres romanguin a disposició de les persones treballadores, la RLPT i la ITSS (art. 34.9 ET).

El Ministeri de Treball, Migracions i Seguretat Social, a la Guia sobre el registre de jornada, va indicar que aquesta obligació establerta en la normativa havia de ser interpretada en el sentit que sigui possible accedir als registres en qualsevol moment en què siguin sol·licitats; havent de romandre físicament en el lloc de treball o ser accessibles des del mateix de forma immediata (tenint en compte que aquesta possibilitat d'accés i consulta de la informació no implica l'obligació de lliurament de còpies del registre).

No obstant això, l'Audiència Nacional, en la seva Sentència núm. 168/2024, de 9 de desembre de 2024, va rebutjar el criteri no vinculant establert pel Ministeri de Treball,

Migracions i Seguretat Social, considerant que de la normativa (art. 34.9 ET) no es desprèn l'obligació de posar a disposició de la RLPT un sistema d'accés immediat als registres de jornada. En el supòsit descrit la RLPT havia pactat amb l'empresa que la informació seria lliurada de forma mensual, concloent l'Audiència Nacional que aquest sistema de posada a disposició no contravenia la normativa.

L'Audiència Nacional va reiterar aquest criteri en la Sentència núm. 28/2025, de 24 de febrer de 2025, argumentant que no podia exigir-se un sistema d'accés i posada a disposició immediat quan la norma no ho preveu i la RLPT havia acordat amb l'empresa la possibilitat de verificar per períodes regulars els resultats del registre de la jornada.

En definitiva, l'article 34.9 de l'Estatut dels Treballadors no imposa expressament l'obligació de facilitar la informació de manera immediata. Tanmateix, això no impedeix que la RLPT pugui pactar amb l'empresa un accés immediat a aquesta informació. Així es desprèn del supòsit descrit en la Sentència del Tribunal Suprem núm. 777/2024, de 16 de setembre de 2025, en què sindicats i empresa havien acordat que s'habilitaria un sistema perquè la RLPT pogués accedir al registre diari de les persones treballadores en qualsevol moment i una vegada tancat el marcatge anterior. No havent proporcionat l'empresa la informació sol·licitada, el Tribunal Suprem conclou que s'havia produït una vulneració del dret a la llibertat sindical.

A quina informació relativa al registre de jornada ha de la RLPT tenir accés?

Amb l'objectiu de garantir que la RLPT pugui exercir les seves funcions de control del compliment de la normativa laboral, l'Estatut dels Treballadors estableix que els registres romandran a la seva disposició.

No obstant això, l'Estatut dels Treballadors no concreta a quina informació ha de tenir accés la RLPT. En tot cas, cal tenir en compte que, en la transmissió de la informació, la jurisprudència pondera el dret de la RLPT a la informació amb la salvaguarda del dret a la protecció de dades de les persones treballadores.

Sobre aquesta qüestió es va pronunciar l'Audiència Nacional, en la seva Sentència núm. 57/2022, de 19 d'abril de 2022, confirmada per la Sentència del Tribunal Suprem núm. 1161/2024, de 24 de setembre de 2024, en la qual va reconèixer que la transmissió de la identitat (nom i cognoms), província i població de les persones treballadores associades a cada registre de jornada no suposava una vulneració del dret a la protecció de dades. El seu lliurament venia justificat, ja que, de denegar aquesta informació les funcions de vigilància i control de la RLPT es veurien minvades.

Té la RLPT dret a ser consultada sobre la forma d'organització i documentació del sistema de registre de jornada? I a negociar-ne el contingut?

L'empresa pot decidir la forma d'organitzar i documentar el sistema de registre de jornada. No obstant això, davant d'aquesta decisió —o davant d'una modificació en la manera d'organització i documentació del registre—, la RLPT haurà de ser consultada (art. 34.9 ET). L'incompliment del deure de 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 ITSS 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).

Igualment, en tot cas, mitjançant conveni col·lectiu o acord d'empresa, la RLPT pot negociar la implantació d'un mecanisme concret d'organització i documentació del sistema de registre (art. 34.9 ET), que haurà de ser respectat per l'empresa, la qual restarà vinculada al que s'estableixi en el conveni.

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).

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)²¹.
4. Dret de consulta sobre la manera d'organització i documentació del sistema de registre de jornada (art. 34.9 ET).
5. Dret d'informació sobre les dades del registre de jornada (art. 34.9 ET).
6. Dret d'informació sobre els riscos identificats en el lloc de treball i les mesures i activitats de protecció i prevenció aplicades (art. 18.1 LPRL).
7. Dret d'informació sobre els mecanismes de prevenció que s'utilitzin a l'empresa (art. 64.2.d) ET).
8. Dret de consulta sobre la implementació de noves tecnologies en el lloc de treball en tot allò relacionat amb les conseqüències que aquestes poguessin tenir per a la seguretat i salut de les persones treballadores (art. 33.1.a) LPRL).

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

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'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 documentació assenyalades en l'apartat 1 de l'article 18 i en

²¹ 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).

l'apartat 1 de l'article 23 de la Llei de Prevenció de Riscos Laborals (art. 12.19 LISOS).

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

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

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

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

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

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

En aquests supòsits, davant una potencial lesió del dret a la llibertat sindical a causa de la inobservança dels drets d'informació i consulta, els sindicats afectats podran presentar demanda de tutela de drets fonamentals 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).

4. 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.

4.1. Davant la videovigilància, la gravació de so i el GPS al treball

Consentiment de la persona treballadora

La llei permet a l'empresa instal·lar càmeres i sistemes de geolocalització sense demanar el consentiment exprés de les persones treballadores, perquè s'entén que la mesura es troba justificada per l'existència d'una relació laboral (com s'explica en els apartats 2.1 i 2.2 de la guia).

No obstant això, encara que la llei no requereixi el consentiment de les persones treballadores, el conveni col·lectiu pot **establir garanties addicionals**. Es recomana incloure una clàusula que exigeixi el **consentiment exprés de la persona treballadora** per a la captació d'imatges i la recopilació de les dades de localització, com a mesura de protecció reforçada de la intimitat.

Justificació estricta i ús excepcional

El conveni pot exigir que la instal·lació de sistemes de videovigilància i geolocalització sigui una **mesura excepcional**. L'empresa hauria de **justificar per escrit** la necessitat concreta de les càmeres i els GPS. Només s'haurien de permetre en els **supòsits expressament previstos** al conveni.

Es pot establir que, fora d'aquests supòsits, **no existeix interès legítim empresarial** per gravar o registrar la ubicació.

Prohibició al teletreball

La Llei de Treball a Distància reconeix que, en la utilització dels mitjans telemàtics i el control de la prestació laboral mitjançant dispositius automàtics, s'haurà de respectar el dret a la intimitat i a la protecció de dades. No obstant això, no prohibeix expressament l'establiment de sistemes de control que capten imatges o graven sons i que poden ser especialment intrusius quan la persona treballadora desenvolupa l'activitat laboral en el seu domicili.

Es recomana **prohibir expressament** l'ús de càmeres o fotografies o sistemes de gravació de sons per controlar l'activitat laboral en el **treball a distància**. El domicili i els espais privats mereixen una protecció reforçada.

Prohibició d'ús fora de la jornada laboral

Com a regla general, el control empresarial mitjançant dispositius digitals o tècniques de Videovigilància està prohibit fora del temps de treball. Aquesta prohibició inclou expressament sistemes com el GPS, la geolocalització mitjançant dispositius mòbils o altres mitjans de vigilància electrònica. El fonament jurídic d'aquesta regla es troba en el dret fonamental a la intimitat personal i familiar i a la protecció de dades personals, així com en la limitació del poder de direcció empresarial al temps de prestació efectiva de serveis (art. 18 CE; art. 20.3 ET; arts. 87 a 90 LOPDGDD; art. 6 i 88 RGPD).

Tanmateix, la jurisprudència no ha estat absolutament uniforme. Algunes resolucions judicials han admès, la vigilància electrònica fora del temps de treball i han considerat vàlida la prova obtinguda mitjançant aquests mecanismes.

Aquesta doctrina jurisprudencial genera un marge d'incertesa jurídica. Precisament per això, els convenis col·lectius poden pactar la prohibició absoluta de l'ús de mitjans de vigilància electrònica fora del temps de treball, sense excepcions.

Si el conveni col·lectiu estableix una prohibició clara i inequívoca, el control mitjançant dispositius electrònics fora del temps de treball no només seria il·lícit, sinó que també es veuria reforçada la seva inadmissibilitat com a prova en un procediment judicial.

Informació clara sobre la finalitat de les càmeres

L'empresa, quan instal·la un sistema de videovigilància, ha d'informar les persones treballadores sobre la finalitat per a la qual s'utilitzaran les càmeres. No obstant això, tal com s'explica detalladament a l'apartat 2.1 de la guia, la pròpia normativa permet utilitzar, amb finalitats disciplinàries, les imatges captades per càmeres sobre les quals no s'ha informat de la seva finalitat de control, quan s'hagi captat la comissió flagrant d'un acte il·lícit.

Per a garantir la transmissió d'una informació detallada i completa en tot cas, és recomanable que el conveni obligui l'empresa a informar de manera clara i prèvia sobre:

- Per què s'instal·len les càmeres.
- Si són per seguretat o per control laboral.
- Quines conseqüències poden tenir les gravacions.

Tot i això, cal advertir que, segons els tribunals, l'empresa **no perd el poder disciplinari** encara que inicialment digui que les càmeres no s'usaran per sancionar.

Informació obligatòria a la representació legal

El conveni pot reforçar la transparència establint que **sempre** s'ha d'informar a la representació legal de les persones treballadores i establint, expressament, la **nul·litat** de les proves obtingudes mitjançant el sistema de videovigilància o geolocalització en cas contrari.

La representació legal hauria de ser informada, en tot cas, sobre:

- La implantació de càmeres i GPS.
- Les modificacions del sistema.
- Els canvis de finalitat de l'ús del sistema de vigilància (principalment informar sobre si té finalitat disciplinària o no).

Registre de càmeres i GPS

Per a garantir la transparència i la seguretat en l'ús de les càmeres i els GPS 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 intern de sistemes de videovigilància o geolocalització**, que inclogui la següent informació:

- Tipus de càmeres o GPS.
- Ubicació exacta.
- Finalitat.
- Possible impacte laboral.

La representació legal hauria de tenir **accés al registre**. El registre s'ha d'actualitzar davant qualsevol canvi, per exemple, davant un canvi d'ubicació de les càmeres.

Prohibició general de gravació de veu

La llei únicament permet la gravació de sons quan existeixen riscos rellevants per a la seguretat de les instal·lacions, béns i persones derivats de l'activitat que es desenvolupa en el centre de treball. No obstant això, tal com s'indica en l'apartat 2.1 de la guia, en l'àmbit d'empreses de **call-centre** o **telemàrqueting** la jurisprudència sí que sembla admetre la gravació de les converses i crides realitzades per les persones treballadores amb els clients degut a la naturalesa de la prestació del servei.

Per a garantir una major protecció de la intimitat de les persones treballadores de sectors de telemàrqueting, el conveni pot establir que:

- Les gravacions siguin **puntuals i no generals**.
- L'empresa hagi de demostrar que **no existeixen alternatives menys invasives**.

En qualsevol cas, és recomanable que amb caràcter general es prohibeixi la gravació de veu, tret que existeixin riscos greus per a la seguretat de persones o instal·lacions.

Garanties en gravacions ocultes

Encara que la llei exigeix que les persones treballadores tinguin almenys coneixement de l'existència de les càmeres perquè l'empresa pugui tractar les imatges obtingudes de les gravacions, la jurisprudència sí que ha legitimat el control ocult en determinats supòsits

en què hi havia sospites fundades i raonables de greus irregularitats laborals (apartat 2.1 de la guia).

El conveni pot exigir que, en aquests casos excepcionals de gravació oculta, es garanteixi la **participació de la representació sindical** durant el procés, provocant la nul·litat de les proves quan no hi va haver participació de la representació sindical.

Això reforça el control col·lectiu i evita abusos.

Reducció del temps de conservació

Encara que la llei permet conservar imatges fins a **un mes**, el conveni pot:

- Reduir aquest termini al **mínim imprescindible**.
- Permetre arribar al màxim legal només en casos degudament justificats.

En el cas dels GPS, atès que la normativa no fixa un termini màxim clar de conservació de les dades, el conveni pot establir-lo. Les dades obtingudes mitjançant el sistema de geolocalització s'haurien de conservar:

- Només durant el temps **imprescindible** i, com a màxim, durant dos mesos.
- Exclusivament per a la finalitat que justifica el control. Un cop passada aquesta finalitat, les dades s'han d'eliminar.

Prohibició d'obligar a utilitzar dispositius personals

En l'apartat 2.2 de la guia s'indica que l'empresa no pot, en principi, obligar unilateralment la persona treballadora a aportar un dispositiu digital de la seva propietat per instal·lar un sistema de geolocalització. Aquesta mesura constitueix un abús de dret empresarial, contrari a la nota d'alienitat que caracteritza les relacions laborals.

El conveni pot recordar i reforçar que la persona treballadora no està obligada a utilitzar dispositius propis per instal·lar una aplicació que permeti conèixer la seva localització. No es pot exigir descarregar aplicacions que registren la ubicació de les persones treballadores en telèfons o ordinadors personals.

Només es podria permetre de manera voluntària, amb autorització de l'empresa i acceptació expressa de la persona treballadora.

Prohibició de combinar tecnologies invasives

Els sistemes de videovigilància poden ser complementats amb altres tecnologies que poden permetre a l'empresa obtenir més dades de les persones treballadores, accedir a informació sensible o automatitzar processos sense intervenció humana. Aquestes tecnologies poden ser especialment invasives, per això, el conveni hauria de prohibir expressament que les càmeres incorporin:

- Reconeixement facial.
- Anàlisi d'expressions o moviments.
- Elaboració de perfils automatitzats.
- Decisions automatitzades basades en imatges.

La combinació d'aquestes tecnologies amb càmeres podria declarar-se al conveni com a **desproporcionada i il·lícita**. En l'apartat 2.1.1 de la guia es descriuen les prohibicions que ja recull la normativa europea.

4.2. Davant el registre de dispositius electrònics

Acord obligatori sobre la política d'ús dels dispositius electrònics

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

El conveni col·lectiu pot reforçar aquesta obligació. Es recomana establir que aquesta política no pugui ser decidida unilateralment per l'empresa. La política d'ús hauria de ser **negociada i acordada** amb la representació de les persones treballadores. D'aquesta manera es garanteix que les normes siguin clares, conegudes i acceptades per tota la plantilla.

Restricció estricta de les causes que justifiquen el control

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

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

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

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

Prohibició del control permanent o continu

Es recomana prohibir els sistemes de monitorització constant dels dispositius electrònics. El control continu genera una pressió permanent i afecta la intimitat de la persona

treballadora. El conveni pot establir que el control sigui sempre puntual, limitat en el temps i vinculat a una causa concreta, pactant expressament la nul·litat de qualsevol prova recollida fora dels supostos pactats.

.

Prohibició de la intercepció de les comunicacions

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

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

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

Protecció reforçada davant sistemes basats en intel·ligència artificial

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

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

Registre dels dispositius electrònics existents a l'empresa

La llei obliga l'empresa a elaborar uns criteris d'ús dels dispositius electrònics amb la participació de la representació legal, i a informar del seu contingut a les persones treballadores. Aquests criteris, tal com s'explica en l'apartat 2.4 de la guia, hauran

d'indicar almenys les prohibicions d'ús absolutes o parcials, la possibilitat que l'empresa realitzi un registre dels dispositius amb finalitats de control i les eines de control que podrien ser emprades per l'empresa.

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

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

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

Ús personal raonable dels mitjans tecnològics

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

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

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

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

Presència de la representació de les persones treballadores

Segons s'exposa en l'apartat 2.4 de la guia, en principi, l'empresa podrà accedir al contingut dels dispositius digitals quan així estigui previst en els criteris d'ús, existeixi una raó que legítimi el registre i es respecti el principi de proporcionalitat. No obstant

això, encara que es compleixin les garanties establertes en la llei, l'accés als dispositius digitals pot constituir una pràctica intrusiva per a la intimitat de les persones treballadores.

Per això, en empreses amb especial risc de control excessiu, el conveni pot introduir **garanties addicionals**. Una d'elles pot ser permetre o exigir la **presència** de la **representació sindical** durant els processos de monitorització o revisió dels dispositius electrònics.

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

Transparència reforçada sobre la política de control

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

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

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

Limitació del tipus de dades que poden ser recollides

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

S'hauria de prohibir la recollida de dades sobre:

- Hàbits personals.
- Preferències.
- Estat emocional.

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

Limitació del temps de conservació de les dades

Atès que la normativa no fixa un termini màxim clar de conservació de les dades, el conveni pot establir-lo. Es podria pactar que les dades obtingudes mitjançant el control dels dispositius electrònics no s'haurien de conservar més temps que el permès per la prescripció de les infraccions establerta al estatut dels treballadors que es en tot cas de 6 mesos (art. 60 ET)

Prohibició de combinar el control digital amb altres tecnologies invasives

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

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

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

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

4.3. Davant el registre de jornada

Concreció clara de com s'ha de fer el registre de jornada

La llei no estableix una forma expressa en la qual s'hagi d'efectuar el registre de jornada. Així, el conveni col·lectiu pot definir de manera concreta com s'ha de realitzar el registre horari. No n'hi ha prou amb dir que s'ha de registrar l'entrada i la sortida. Cal establir pautes clares perquè el sistema sigui fiable i respectuós amb el dret a la protecció de dades de la persona treballadora. El registre ha de recollir únicament informació laboral i evitar dades innecessàries o excessives.

Acord amb la representació sobre el contingut del registre

La llei únicament indica, com s'assenyala en l'apartat 3 de la guia, que l'organització i documentació del registre podrà ser concretada mitjançant negociació col·lectiva o acord d'empresa o, en defecte d'això, decisió de l'empresari prèvia consulta amb els representants legals de les persones treballadores.

El conveni pot establir expressament que el registre de jornada s'hagi de acordar amb la representació legal per a evitar que s'implanti el sistema per decisió unilateral de l'empresari.

I aquest hauria d'incloure com a mínim:

- Dades de la persona treballadora i de l'empresa.
- Dia concret.
- Hora real d'entrada i de sortida.
- Descansos, si n'hi ha.
- Jornada ordinària pactada.
- Hores ordinàries, complementàries i extraordinàries, desglossades per dia.
- Signatura de la persona treballadora i de la representació legal.

S'hauria de prohibir el sistema en paper o emplenar registres amb posterioritat per a garantir la fiabilitat de les dades registrades i evitar que es puguin manipular.

Anonimització de les dades personals

Els sistemes de registre de jornada han de vincular les dades registrades relatives a l'horari amb la persona treballadora que correspongui, per això contenen i recopilen informació personal.

Tanmateix, el conveni pot establir sistemes de registre horari més garantistes mitjançant l'ús de codis d'identificació en lloc del nom i cognoms.

Aquesta mesura redueix riscos per a la protecció de dades. Tot i això, es pot deixar clar que tant l'ús de noms com de codis és vàlid, sempre que el sistema sigui segur i proporcional.

Prohibició de formes de registre invasives per a la intimitat

En l'apartat 2.5 de la guia s'explica que la llei no fixa un sistema concret de registre de jornada, però que, depenent del sistema implementat, es pot veure afectat el dret a la intimitat i/o el dret a la protecció de dades de les persones treballadores. Hi ha sistemes que poden ser més invasius perquè es complementen amb tecnologies que capten dades addicionals de les persones treballadores (per exemple, el rostre, la localització, etc.).

El conveni pot excloure expressament determinades formes de registre de jornada que siguin especialment intrusives. Si el sistema exigeix l'ús de videovigilància, geolocalització o dispositius digitals, s'han de respectar estrictament els drets d'intimitat i protecció de dades. El conveni pot descartar aquells controls de presència que resultin sospitosos o desproporcionats, és a dir, que no siguin realment necessaris per al compliment de l'obligació o que causen uns perjudicis per als drets de les persones treballadores que no es corresponen amb els beneficis que proporciona el sistema.

Prohibició de l'ús de la veu com a sistema de registre

El conveni deuria prohibir expressament el registre de jornada basat en la veu de la persona treballadora. Les gravacions de veu i converses són una mesura molt intrusiva. En l'apartat 2.5 de la guia s'indica que aquest tipus de control no supera generalment el principi de proporcionalitat (principis de necessitat, idoneïtat i proporcionalitat en sentit estricte) i afecta greument la intimitat i la protecció de dades.

Prohibició de microxips o dispositius implantats al cos

El conveni pot prohibir de manera clara qualsevol sistema de registre que impliqui la implantació de microxips sota la pell.

Aquestes pràctiques són extremadament invasives. Existeixen mitjans molt menys intrusius per complir la mateixa funció, fet que les fa injustificables.

Prohibició d'obligar a utilitzar dispositius personals

En l'apartat 2.5 de la guia s'indica que l'empresa no pot, en principi, obligar unilateralment la persona treballadora a aportar un dispositiu digital de la seva propietat per al compliment d'una obligació de registre. Aquesta mesura constitueix un abús de dret empresarial, contrari a la nota d'alienitat que caracteritza les relacions laborals.

El conveni pot recordar i reforçar que la persona treballadora no està obligada a utilitzar dispositius propis per a complir amb l'obligació legal de registrar la jornada. No es pot exigir instal·lar aplicacions de registre de jornada en telèfons o ordinadors personals.

Només es podria permetre de manera voluntària, amb autorització de l'empresa i acceptació expressa de la persona treballadora.

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.

Accés directe de la persona treballadora al seu registre

El conveni pot establir que la persona treballadora rebi el seu registre de jornada de manera automàtica. No hauria de ser necessari demanar-lo. Es pot pactar una periodicitat concreta perquè cada persona tingui còpia del seu registre.

Determinació clara del sistema de lliurament del registre

D'acord amb la normativa, els registres han de romandre a disposició de les persones treballadores. El conveni pot indicar quin serà el sistema tecnològic utilitzat per accedir al registre. Aquest sistema ha de ser senzill, accessible i comprensible.

Entrega periòdica del registre a la representació legal

Si bé l'empresa té el deure de garantir que els registres de jornada romanguin a disposició de la representació legal, la normativa no concreta com ha de ser transmesa la informació (explicació recollida en l'apartat 3 de la guia).

El conveni pot reforçar el dret d'accés de la representació legal establint una entrega periòdica, per exemple, mensualment i en format informàtic. També es pot regular, expressament, la possibilitat de consulta immediata.

La informació ha d'incloure el còmput total d'hores de cada persona treballadora. Aquesta mateixa informació es pot facilitar als delegats i delegades sindicals dins del seu àmbit de representació.

Intervenció de la representació legal en cas de discrepàncies

El conveni pot establir mecanismes clars per resoldre discrepàncies en el registre de jornada. La persona treballadora ha de poder consultar i revisar el seu registre. La representació legal pot intervenir per verificar possibles errors i establir mecanismes al conveni col·lectiu per a que la representació legal accepti o no la validesa del contingut del registre de forma periòdica. De aquesta forma, la representació legal podrà deixar registrada la existència de conflictes o impugnacions al establert al registre de jornada.

Desenvolupament del dret de rectificació

En concordança amb el que s'acaba de veure, el conveni pot reforçar el dret de la persona treballadora a corregir errors en el registre. S'hauria d'indicar clarament a quin departament o responsable s'ha d'adreçar la reclamació. També es poden fixar terminis per donar resposta i corregir les dades incorrectes.

4.4. 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, es recomanable establir la nul·litat de qualsevol informació obsessa mitjançant aquestes sistemes que siga 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 salut de la persona treballadora. A més de nou, es molt important que se pacte que qualsevol ús de aquestes dades per a finalitats diferents de la prevenció, i especialment per a finalitats disciplinàries, 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'eliminïn 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 capacitat 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'ús 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'ús de qualsevols sistema de control per part de l'empresa que no siga informat a la plantilla de l'empresa.

Avaluació prèvia d'impacte sobre drets

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

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

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