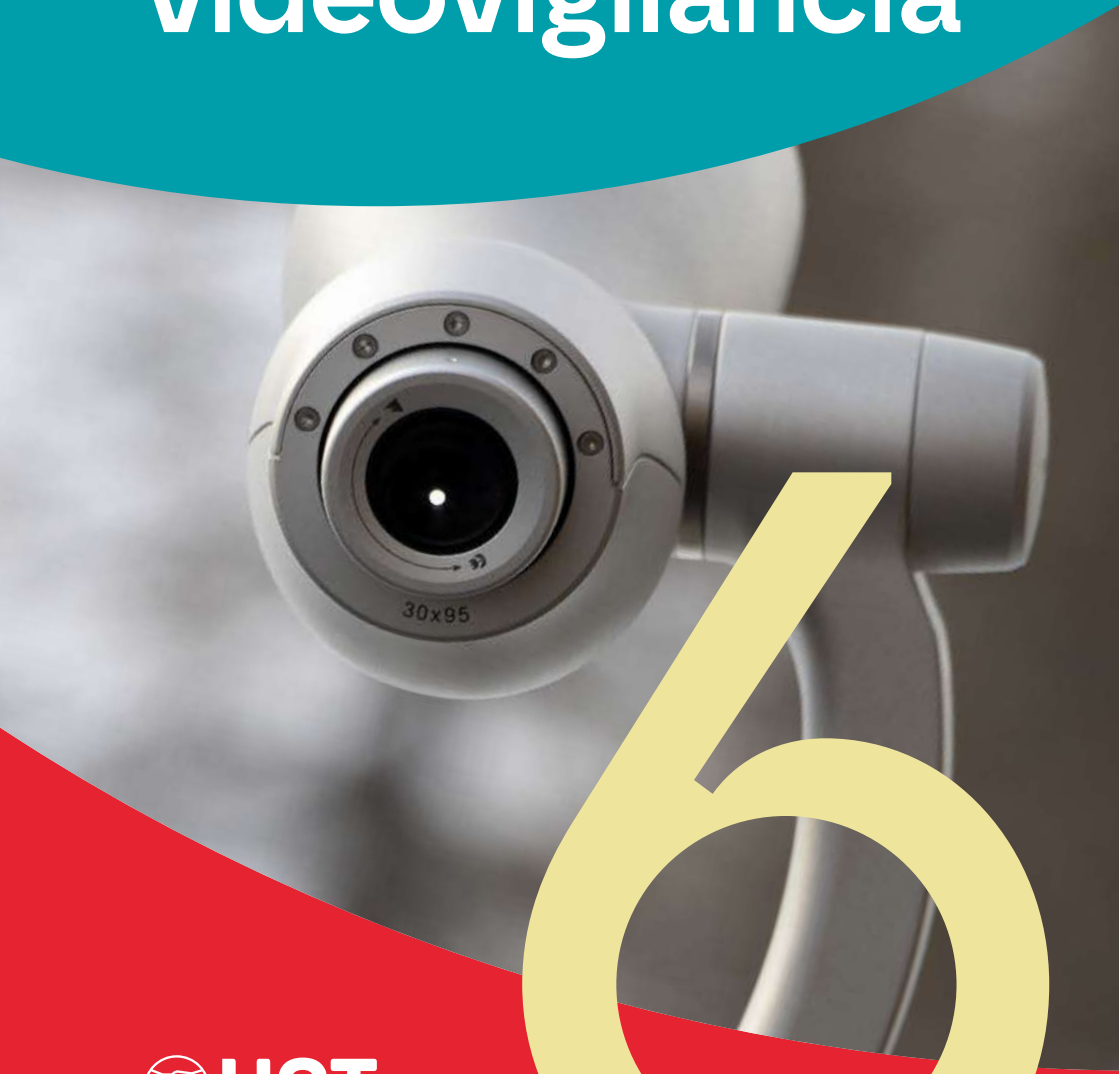
Guia de drets laborals i de prevenció de riscos: IA i vigilància tecnològica

Sistemes de videovigilància



6

UGT.cat

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

Sistemes de videovigilància

Edició:
UGT de Catalunya
2026

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

Alba Navalón Arnal,
Universitat de València.

Disseny i maquetació:
Manera Estudi

Fotografies:
Magnific

Impressió:
Impremta Pagès

Dipòsit legal:
B 11746-2026

Amb el suport de:

UGT.cat

a la feina cap risc

Generalitat de Catalunya

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

Sistemes de videovigilància

Taula de continguts

Presentació

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

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

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

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

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

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

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

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

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

Oscar Riu i Garcia

Secretari Política Sindical de la UGT de Catalunya

Reyes Solaz

Secretària Nacional UGT de Catalunya-Salut Laboral

Introducció

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Drets individuals en matèria de privacitat i prevenció de riscos laborals

Davant 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 demostri 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,

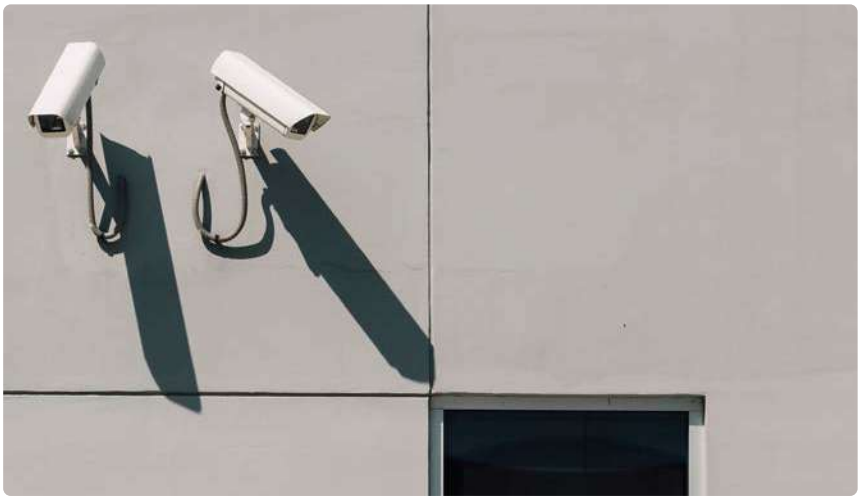
de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (art. 89.1, paràgraf segon, LOPDGDD).

En primer lloc, respecte a l'expressió "comissió flagrant", s'ha d'entendre que aquesta inclou tant les troballes casuals 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 –deixa-



desa 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 aporti 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'hagi 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).

L'incompliment de la normativa sobre videovigilància laboral pot vulnerar els drets a la intimitat i a la protecció de dades de les persones treballadores, que poden reclamar judicialment el cessament de la mesura, indemnitzacions per danys morals i, fins i tot, la nul·litat o improcedència d'un acomiadament basat en proves obtingudes il·lícitament.

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'actuació[1]). Les autoritats podran iniciar un procediment sancionador si consideren que hi ha indicis d'infracció. En aquests supòsits, les sancions que poden ser imposades a les empreses són les següents:

- Multes administratives de 20.000.000 euros com a màxim o d'una quantia equivalent al 4 % com a màxim del volum de negoci total anual global de l'exercici financer anterior, i s'optarà per la de més quantia (art. 83.5 RGPD).
- Aquestes multes es podran aplicar quan es cometin, entre d'altres, les següents infraccions (art. 72.1 LOPDGDD):
  - El tractament de dades personals vulnerant els principis i garanties de l'article 5 del RGPD.
  - El tractament de dades personals sense que es doni alguna de les condicions de licitud del tractament de l'article 6 del RGPD.
  - El tractament de dades personals de les categories de l'article 9 del RGPD sense que es doni alguna de les circumstàncies previstes en aquest precepte.
  - L'omissió del deure d'informar dels articles 13 i 14 del RGPD.
  - L'impediment o l'obstaculització o la no atenció reiterada de l'exercici dels drets establerts als articles 15 a 22 del RGPD.
  - L'incompliment de les resolucions dictades per l'autoritat de protecció de dades.

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

- 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, 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 siguen 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 depressió[2].

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.

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).

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.

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).

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'índole laboral o la promoció o rescissió de relacions contractuals d'índole laboral, per a l'assignació de tasques a partir de comportaments individuals o trets o característiques personals o per supervisar i avaluar el rendiment i el comportament de les persones en el marc d'aquestes relacions". Dins d'aquesta definició 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 avaluació[3] 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 sistema que es pretén implementar no són desproporcionats en relació amb l'objectiu perseguit.

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

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.

L'empresa ha d'informar prèviament i de manera clara sobre la videovigilància amb IA i l'ús de les dades, especialment si es tracta d'IA d'alt risc.

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.

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).

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

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

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

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

La introducció de mitjans tecnològics en el lloc de treball, com sistemes de videovigilància, geolocalització o control algorítmic pot tenir una repercussió negativa sobre la seguretat i salut de les persones treballadores (creant nous perills o potenciant riscos físics o psicosocials ja existents).

Per això, les persones delegades de prevenció hauran de ser consultades sobre la implementació de noves tecnologies en el lloc de treball en tot allò relacionat amb les conseqüències que aquestes poguessin tenir per a la seguretat i salut de les persones treballadores (art. 33.1.a) LPRL). A més, el Comitè de Seguretat i Salut podrà participar en l'elaboració i avaluació dels plans i programes de prevenció de riscos de l'empresa i debatre, a aquest efecte, la introducció de noves tecnologies (art. 39.1.a) LPRL).

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

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

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

1. Dret d'informació i consulta davant la implementació i revisió de sistemes de control del treball (art. 64.5.f) ET).
2. Dret d'informació algorítmica (art. 64.4.d) ET).
3. Dret de participació (consulta) en l'elaboració dels criteris d'utilització dels dispositius digitals (art. 87.3 LOPDGDD)[4].
4. Dret de consulta sobre la manera d'organització i documentació del sistema de registre de jornada (art. 34.9 ET).

4 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).

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

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

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

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

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

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

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

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

Infraccions en matèria de prevenció de riscos laborals:

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

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

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

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

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

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

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

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

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

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

Davant 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 addicio-**

nals. 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.

El conveni pot limitar la videovigilància i la geolocalització a supòsits excepcionals degudament justificats i previstos, i prohibir el control electrònic fora de la jornada laboral i en el teletreball, amb l'objectiu de reforçar la protecció de la intimitat de les persones treballadores.

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'us del sistema de vigilància (principalment informar sobre si te finalitat disciplinaria 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 sistemes 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 declararse 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.


UGT.cat

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

Sistemes de videovigilància

6

UGT.cat