

Judit Galceran López

LA VIDEOVIGILÀNCIA EN L'ÀMBIT LABORAL

TREBALL DE FI DE GRAU

dirigit pel Dr. Jordi Barrat i Esteve

Grau de Relacions Laborals i Ocupació



UNIVERSITAT ROVIRA I VIRGILI

Tarragona

2016

Resum

Aquest treball té com a objecte examinar els conflictes que es plantegen entre la instal·lació de sistemes de videovigilància i la lesió dels drets fonamentals. En ell s'analitza la legislació, jurisprudència i doctrina dictada més rellevant sobre la matèria. Es fa especial referència a la utilització de videocàmeres en l'àmbit laboral.

Resumen

Este trabajo tiene por objeto examinar los conflictos que se plantean con la instalación de sistemas de videovigilancia y la lesión de los derechos fundamentales. En él se analiza la legislación, jurisprudencia y doctrina dictada más relevante sobre la materia. Se hace especial mención a la utilización de videocámaras en el ámbito laboral.

Abstract

This work focuses on examining the conflicts that arise between the installation of video surveillance systems and its infringement on fundamental rights. The article analyzes the main legal materials, particularly legislation and most relevant case law and doctrine. Special mention is made to the use of video surveillance in the workplace.

Paraules clau/ Keywords

VIDEOVIGILÀNCIA – VIDEOCÀMERES – DRETS FONAMENTALS – INTIMITAT – PRÒPIA IMATGE – PROTECCIÓ DE DADES – LLOC DE TREBALL – PROPORCIONALITAT
--

Índex

Índex	3
Llistat de sigles i abreviatures	5
Introducció.....	8
1. La videovigilància	10
1.1 Concepte	10
1.2 Tipus.....	13
1.2.1 Forces i Cossos de Seguretat en lloc públics.....	13
1.2.2 Videovigilància en l'àmbit privat.....	15
1.3 Finalitats	17
1.3.1 Seguretat.....	17
1.3.2 Control empresarial	17
1.3.3 Altres fins.....	19
2. Videovigilància i Drets Fonamentals	20
2.1 Dret a la intimitat personal.....	20
2.1.1 Concepte i evolució	20
2.1.2 Dret a la intimitat en l'àmbit laboral.....	23
2.2 Dret a la pròpia imatge.....	26
2.2.1 El dret a la pròpia imatge en l'àmbit laboral	28
2.3 Dret a la protecció de dades	29
2.3.1 El dret a la protecció de dades en l'àmbit laboral	31
2.4 Llibertat ideològica, el dret de reunió i manifestació, la llibertat sindical i el dret de vaga	33
2.5 Dret al secret de les comunicacions	35
2.6 Dret a la inviolabilitat del domicili	36
3. La videovigilància en l'àmbit laboral	39

3.1 El conflicte entre el poder de direcció de l'empresari i els drets dels treballadors	40
3.2 Requisits.....	42
3.2.1 El principi de proporcionalitat	42
3.2.2 Interès legítim.....	46
3.2.3 Deure d'informació i principi de consentiment	47
3.3 Drets ARCO	50
3.3.1 Dret d'accés	51
3.3.2 Drets de rectificació i cancel·lació	52
3.3.3 Dret d'oposició.....	53
Conclusions	55
Bibliografia.....	58
Webgrafia	61
Annexos	65
Annex I - Model de cartell informatiu segons la Instrucció 1/2006, de 8 de novembre, de l'AEPD	66
Annex II - Models de cartells informatius segons la Instrucció 1/2009, de 10 de febrer, de l'APDCAT	67
Annex III - Escrit per a comunicar als treballadors la instal·lació de càmeres de videovigilància en el centre de treball	68
Annex IV - Escrit per a comunicar als representants dels treballadors sobre la instal·lació de càmeres de videovigilància en el centre de treball.....	69

Llistat de sigles i abreviatures

Sigles

AEPD= Agència Espanyola de Protecció de Dades, Agencia Española de Protección de Datos

AN= Audiència Nacional, Audiencia Nacional

APDCAT= Agència Catalana de Protecció de Dades, Agencia Catalana de Protección de Datos

CE= Constitució Espanyola, Constitución Española

CEDH= Conveni Europeu per a la protecció dels Drets Humans i les llibertats fonamentals (Conveni Europeu de Drets Humans), Convenio Europeo para la protección de los Derechos Humanos y de las libertades fundamentales (Convenio Europeo de Derechos Humanos)

ET= Estatut dels Treballadors, Estatuto de los Trabajadores

LO= Llei Orgànica, Ley Orgánica

LOPH= Llei Orgànica sobre protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge, Ley Orgánica sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen

LOPD= Llei Orgànica de Protecció de Dades, Ley Orgánica de Protección de Datos

LISOS= Llei d'Infraccions i Sancions de l'Ordre Social, Ley sobre Infracciones y Sanciones en el Orden Social

LORTAD= Llei Orgànica de Regulació del Tractament Automatitzat de Dades de Caràcter Personal, Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal

LSP= Llei de Seguretat Privada, Ley de Seguridad Privada

RD= Reial Decret, Real Decreto

RLOPD= Reglament de desenvolupament de la Llei Orgànica de Protecció de Dades,
Reglamento de desarrollo de la Ley Orgánica de Protección de Datos

TC= Tribunal Constitucional, Tribunal Constitucional

TEDH= Tribunal Europeu de Drets Humans, Tribunal Europeo de Derechos Humanos

TS= Tribunal Suprem, Tribunal Supremo

TSJ= Tribunal Superior de Justícia, Tribunal Superior de Justicia

Abreviatures

art.	article
arts.	articles
fj.	fonament jurídic
núm.	número
p.	pàgina
pp.	pàgines
v.	veure, vegeu

Introducció

Aquest Treball de Fi de Grau té com a objecte realitzar un estudi sobre la captació i gravació de la imatge i so mitjançant sistemes de videocàmeres, parant especial atenció en l'àmbit laboral. He escollit aquesta temàtica d'estudi degut a l'interès que em suscita aquesta pràctica desplegada ja en tot tipus d'entorns actualment. L'aparició de les noves tecnologies de la informació i de la comunicació (TIC) ha suposat una vertadera revolució, també en l'àmbit de les relacions laborals. En efecte, cada vegada amb més freqüència s'utilitzen més instruments informàtics que no només optimitzen i faciliten tot tipus de processos de gestió i organització del treball, sinó també de vigilància. En aquest cas, l'instrument de control al qual prestaré atenció és la videovigilància. Aquest nou mecanisme de vigilància genera una problemàtica important en tant que es poden veure afectats varis drets fonamentals com ara la intimitat, la pròpia imatge o la protecció de dades. Per això, la recent extensió d'aquest fenomen en múltiples àmbits, juntament amb el xoc de conflictes que produeix, són els motius que m'han conduït a escollir aquest objecte d'estudi.

L'impacte de la videovigilància ha sigut elevat en tots els aspectes, però estem davant un fenomen gairebé desconegut degut a la seva relativa novetat. En aquest punt, es plantegen els següents interrogants, als quals s'intentarà donar resposta durant el desenvolupament del present estudi: la instal·lació de sistemes de videocàmeres representa una vulneració als drets fonamentals de les persones? I en el marc d'una relació laboral, és legítima la instal·lació de sistemes de videovigilància per al control i vigilància dels treballadors, o bé, en altres termes, preval el poder de direcció de l'empresari o els drets fonamentals dels treballadors?

El treball s'estructura en tres capítols, en els que es tractaran els següents aspectes: en primer lloc, s'abordarà el fenomen de la videovigilància en termes generals, diferenciant entre la que es realitza en l'àmbit públic d'aquella que es realitza en l'àmbit privat, així com els diferents usos i aplicacions que pot tenir; en el segon capítol, es tractaran els diferents drets fonamentals que entren en conflicte amb la videovigilància; i, per últim, el tercer capítol es centrarà específicament en la utilització de les videocàmeres com a instrument de vigilància i control en el marc de les relacions laborals, detallant els requisits que ha de complir l'empresari i el drets ARCO que tenen els treballadors al respecte.

La metodologia d'aquest estudi es centra en un anàlisi des d'una perspectiva jurídic-constitucional de la videovigilància. Això és, un anàlisi de la normativa actual existent de la matèria, així com la doctrina i jurisprudència més rellevant que ha anat dictant el Tribunal Constitucional (a partir d'ara TC) al respecte, fent especial menció a la més recent sentència que ha assentat el TC en matèria de protecció de dades, la qual ha introduït un dràstic gir en el criteri que s'havia vingut considerant fins al moment (STC 39/2016).

Els objectius que es pretenen assolir mitjançant el treball són estudiar l'ús i aplicació de les noves tecnologies de videovigilància com a instrument de vigilància i control en qualsevol entorn, conèixer en profunditat la repercussió que genera aquesta nova forma de vigilància sobre els drets fonamentals, especialment la intimitat, la pròpia imatge i la protecció de dades i investigar les conseqüències jurídiques que comporta tal mesura. Per últim, s'analitzarà els elements que permeten assolir un punt d'equilibri entre el respecte als drets fonamentals dels treballadors i la facultat de vigilància i control de l'empresari i l'ús de les noves tecnologies de la informació en l'empresa.

Aquest Treball de Fi de Grau té especial rellevància per al grau de Relacions Laborals i Ocupació ja que el fenomen de la videovigilància també ha tingut una forta repercussió en el món laboral. Les noves tecnologies s'han introduït en l'àmbit empresarial, aportant múltiples avantatges no només de gestió i organització, sinó també de vigilància. En efecte, l'empresari utilitza la videovigilància com una nova modalitat de vigilància i control, tant amb fins de seguretat i prevenció de delictes com per controlar el compliment dels deures i obligacions laborals durant la prestació del treball. Aquest nou instrument genera una certa problemàtica, en tant que entren en conflicte, d'una banda, el poder de direcció de l'empresari, i de l'altra, els drets fonamentals dels treballadors, principalment la intimitat, la imatge i la protecció de dades.

Per últim, i no menys important, m'agradaria agrair al Dr. Jordi Barrat Esteve la seva direcció i dedicació excel·lent en aquest projecte, que ha estat sens dubte un suport imprescindible. També, donar les gràcies a tota la família i amics pel recolzament i interès rebut en tot moment.

1. La videovigilància

1.1 Concepte

Tal i com reconeix l'Agència Espanyola de Protecció de Dades (a partir d'ara AEPD), la captació i/o tractament de imatges és una pràctica molt estesa en la nostra societat, impulsada pels constants avenços tecnològics i la creixent preocupació per la seguretat pública i privada. Actualment, la vigilància a través de les càmeres de vídeo s'ha convertit en un fenomen omnipresent. És fàcil sentir la mirada de les videocàmeres en supermercats, bancs, gasolineres i una infinitat d'establiments comercials, entitats privades i administracions públiques. Fins i tot en els carrers i carreteres es troben instal·lades abundants videocàmeres que per raons de seguretat o control del tràfic segueixen els moviments dels vianants (RUBIO, 2003, p. 419). D'aquesta manera, s'està fent progressivament realitat el règim panòptic descrit per Bentham com a meditació metafòrica, en el que representa al ciutadà cada vegada més pres perquè es sent vigilat en tot moment, sense saber qui el vigila i sense poder posar cara i ulls a tal vigilant (GOÑI, 2007, p.15).

El concepte de videovigilància fa referència a “tota aquella activitat de vigilància i protecció de les persones i béns exercida a través d'un sistema de seguretat electrònic que combina la gravació i captació de imatges i/o sons” (ETXEBERRIA ET AL., 2011, p. 46). En efecte, la videovigilància implica la captació, i en el seu cas la gravació, d'informació personal en forma d'imatges. Donat que la imatge és una dada personal, la utilització dels sistemes de videovigilància implica el seu sotmetiment a la normativa sobre protecció de dades (ÁLVAREZ, 2014, p. 2).

Les imatges recollides, amb independència del seu format, tenen la consideració de dades personals. En aquest sentit, l'art. 3.a) de la Llei Orgànica 15/1999, de 13 de Desembre, de Protecció de Dades de Caràcter Personal (a partir d'ara LOPD) i l'art. 5.1 del Real Decret 1720/2007, de 21 de Desembre, pel que s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre (a partir d'ara RLOPD) defineixen legalment què constitueix una dada de caràcter personal: “qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus concernent a persones físiques identificades o identificables”. En el mateix sentit es pronuncia l'art. 4.1) del Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'Abril de 2016, relatiu a la protecció de les persones físiques en el

que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades, segons el qual s'entén per dada personal “tota informació sobre una persona física identificada o identificable” (ÁLVAREZ, 2014, p. 2). D'aquesta manera, el concepte de dada personal requereix la concurrència d'un doble element: l'existència d'una informació, i que tal informació es pugui vincular a una persona física identificada o identificable (ÁLVAREZ, 2014, p. 2).

En matèria de protecció de dades, a més de la LOPD i el precitat RLOPD, també ha de tenir-se en compte, degut a la seva importància, la Instrucció 1/2006, de 12 de Desembre, de l'AEPD (a partir d'ara Instrucció 1/2006), sobre el tractament de dades personals amb fins de vigilància a través de sistemes de càmeres o videocàmeres (ÁLVAREZ, 2014, p.2). L'AEPD, en l'exercici de la competència que li atribueix l'art. 37.1.c) de la LOPD, dicta la Instrucció per adequar els tractaments de les imatges amb fins de vigilància als principis de la citada LOPD, i per garantir els drets de les persones les imatges de les quals són tractades per mitjà de tals procediments (Preàmbul Instrucció 1/2006). La Instrucció 1/2006 s'aplica al tractament de dades personals d'imatges de persones físiques identificades o identificables, amb fins de vigilància a través de sistemes de càmeres o videocàmeres (art. 1.1). No obstant, deixa fora del seu àmbit d'aplicació les dades personals d'aquelles imatges que s'hagin obtingut mitjançant la utilització de càmeres i videocàmeres per les Forces i Cossos de Seguretat (art. 1.2), així com el tractament d'imatges realitzades en l'àmbit personal i domèstic (art. 1.3).

D'altra banda, també és rellevant destacar la Instrucció 1/2009, de 10 de Febrer, de l'Agència Catalana de Protecció de Dades (a partir d'ara APDCAT), sobre el tractament de dades de caràcter personal mitjançant càmeres amb fins de videovigilància, que es d'aplicació als tractaments de dades, per ens públics, dins del seu àmbit territorial. Particularment, aquesta contempla de forma específica la possibilitat de captar la dada de la veu dels afectats, aconseguint amb aquesta especificació ajustar-se a una realitat en la que determinats dispositius de videovigilància permeten aquesta captació de la veu (ÁLVAREZ, 2014, p. 2).

Tradicionalment, el sector de la videovigilància ha ocupat els primers llocs en quant a denúncies interposades davant l'AEPD, si bé en l'actualitat, s'han reduït de forma

significativa els procediments sancionadors tot destacant, d'altra banda, l'increment de les advertències (ÁLVAREZ, 2014, p. 1).¹

Els àmbits en els que pot enquadrar-se la videovigilància són múltiples:

“El control i la disciplina del tràfic, la protecció interior i exterior d'immobles pertanyents a les Forces Armades i als Cossos i Forces de Seguretat de l'Estat o la qual vigilància està encomanada als Cossos i Forces de Seguretat, les investigacions realitzades per les unitats de Policia Judicial, la seguretat privada, les relacions jurídico-privades (àmbits laboral, mercantil, sanitari i domèstic), la celebració de judicis i la utilització de videocàmeres pels serveis secrets de l'Estat” (ETXEBERRIA et al., 2011, p.155).

Es poden identificar un infinit número de camps d'aplicació en la videovigilància, encara que aquests es poden reduir en dos grans grups: el públic i el privat, els quals seran tractats més endavant. Cadascun d'aquests àmbits presenta característiques pròpies i requereix d'un enfocament particularitzat, però aplicant tal concepte a l'àmbit laboral, estem davant un mecanisme de control i vigilància consistent en un sistema de gravació d'imatges i captació de sons utilitzat per l'empresari en el centre de treball (ETXEBERRIA ET AL., 2011, p. 155).

La videovigilància no fa referència a un dispositiu concret, sinó que el seu terme abraça una àmplia gamma de sistemes de vigilància mitjançant càmeres, amb solucions tècniques molt diverses que estan en continu desenvolupament. Aquestes modalitats tècniques es poden ordenar de menor a major en funció del seu grau d'intromissió en els drets fonamentals:

- “En el nivell menys agressiu es troba la simple observació física d'un espai per una persona que controla un o varis monitors;
- A continuació es situa l'observació amb gravació simultània d'imatges;
- En tercer lloc es troben els sistemes que permeten la individualització de les persones observades mitjançant zoom en pantalla o ampliació posterior de la imatge;
- En l'últim nivell, i en conseqüència el més agressiu, es troben els sistemes intel·ligents de videovigilància que permeten el reconeixement facial, de la veu o de la matrícula dels vehicles, etc.” (ETXEBERRIA ET AL., 2011, p. 156).

De fet, amb encert s'ha assenyalat que la videovigilància és probablement la mesura restrictiva de drets que es capaç d'afectar a una gamma més extensa de drets

¹ L'AEPD no és l'organisme competent per autoritzar la instal·lació de càmeres de videovigilància, ni en l'àmbit privat ni en el públic. La seva missió és vetllar per la protecció de la imatge com a dada personal, exigint el compliment de la normativa sobre protecció de dades.

fonamentals, de manera que ja no pot considerar-se, des d'una perspectiva jurídic-constitucional o iusfundamental, com la mera juxtaposició de dos supòsits de fet ja coneguts (la captació de la imatge i la captació del so) (ARZOZ, 2002, p. 134). Aquesta eina presenta una potencialitat restrictiva de drets fonamentals que opera en una doble dimensió: d'una banda, com a intromissió en drets relatius a la protecció de la vida privada, els quals es troben agrupats a l'art. 18 de la Constitució Espanyola, de 1978 (a partir d'ara CE) (dret a la intimitat personal, a la pròpia imatge, a la inviolabilitat del domicili, al secret de les comunicacions i a la protecció de dades personals davant la informàtica), i de l'altra, com a obstacle de diversos drets de llibertat, entre els quals s'hi pot incloure la llibertat ideològica (art. 16 CE), la llibertat sindical i el dret de vaga (art. 28 CE) i el dret de reunió i manifestació (art. 21 CE) (ETXEBERRIA ET AL., 2011, p. 158).

1.2 Tipus

Aprofundint en els tipus de videovigilància, és necessari distingir entre aquella utilitzada per les Forces i Cossos de Seguretat en llocs públics i aquella que es produeix en l'àmbit privat.

1.2.1 Forces i Cossos de Seguretat en lloc públics

Una primera distinció bàsica és la videovigilància realitzada per les Forces i Cossos de Seguretat (estatals, autonòmics i locals, en el seu cas), que es troben en llocs públics. Aquests casos compten amb una regulació específica i pròpia, això és la Llei Orgànica 4/1997, de 4 d'Agost, per la que es regula la utilització de videocàmeres per les Forces i Cossos de Seguretat en els llocs públics (a partir d'ara LO 4/1997) i el respectiu Reial Decret 596/1999, de 16 d'Abril que la desenvolupa (a partir d'ara RD 596/1999).²

Aquesta matèria rep el tractament major de LO degut a que afecta directament a drets i llibertats fonamentals, com són l'art. 18.1 CE (dret a la intimitat i a la pròpia imatge) i

² Les Forces i Cossos de Seguretat, segons estableix l'art. 2 Llei Orgànica 2/1986, de 13 de Març, de Forces i Cossos de Seguretat, són: 1) Les Forces i Cossos de Seguretat de l'Estat dependents del Govern de la nació; 2) Els Cossos de Policia dependents de les Comunitats Autònomes; i 3) Els Cossos de Policia dependents de les Corporacions Locals.

18.2 CE (inviolabilitat del domicili, en cas de que, amb els avenços tècniques indiscutibles, les imatges que es captin puguin ser de l'interior d'un domicili), i l'art. 21 CE (dret de reunió i manifestació, ja que el fet de que es produeixin en la via pública no autoritza a que les Forces i Cossos de Seguretat coneguin qui participa en elles) (IZUEL, 2004, p. 2).

És una llei d'abast general, aplicable només als dispositius de control policial instal·lats en llocs públics, que té per objecte imposar límits al ús d'aquests mitjans de gravació d'imatges i sons per garantir i no perjudicar en excés els drets dels afectats, encara que la seva finalitat declarada és la de contribuir a assegurar la convivència ciutadana, la eradicació de la violència i la utilització pacífica de les vies i espais públics, així com prevenir la comissió de delictes, faltes i infraccions relacionades amb la seguretat pública (art. 1.1) (GOÑI, 2007, p. 21-22).

Un aspecte de gran interès en la referida LO és el règim de garanties dels drets fonamentals i llibertats públiques dels ciutadans, que han de respectar-se necessàriament durant la gravació d'imatges i sons per les videocàmeres, i els trets essencials del qual són: el sotmetiment de la instal·lació i ús de les videocàmeres a un règim d'autorització, que s'atorga per un òrgan administratiu, previ informe d'un òrgan col·legiat presidit per un magistrat, informe que serà vinculant si és negatiu (art. 3); l'aplicació del principi de proporcionalitat en la seva doble versió d'idoneïtat i d'intervenció mínima, com a criteri d'adopció de la mesura (art.6); la utilització de les videocàmeres requerirà l'exigència d'un risc raonable per a la seguretat ciutadana (en el cas de les fixes) o d'un perill concret (en el cas de les mòbils) (art.6.4); l'obligació de destruir les gravacions en el termini màxim d'un mes des de la seva captació, excepte que es relacionin amb infraccions penals o administratives greus o molt greus en matèria de seguretat pública, amb una investigació policial o procediment judicial obert (art. 8.1); aquella persona que tingui accés a les gravacions haurà de respectar la deguda discreció i confidencialitat (art.8.2); el deure d'informar al públic de manera clara i permanent de l'existència de videocàmeres fixes, sense especificar el seu emplaçament, i de l'autoritat responsable de la seva instal·lació (art. 9.1) i el reconeixement dels drets d'accés i cancel·lació de les gravacions (art. 9.2) (GOÑI, 2007, p. 23).

La videovigilància pública practicada per les Forces i Cossos de Seguretat es pot donar en diferents camps d'aplicació, com són:

“La seguretat pública en hospitals, edificis i oficines públiques, parcs, jardins, places i qualsevol altre espai obert al públic, així com museus, transports públics i avingudes, la lluita contra la corrupció, les investigacions policials, com a evidència en processos jurisdiccionals, control de la vialitat i el trànsit, prevenció d'emergències i riscos naturals, atenció d'urgències i emissió d'alarmes, auxili dels serveis de protecció civil, treballs d'intel·ligència per part de les autoritats i persecució d'actes il·lícits en qualsevol àmbit” (IBARRA, 2011, p. 258).

1.2.2 Videovigilància en l'àmbit privat

D'altra banda, la nova Llei 5/2014, de 4 d'Abril, de Seguretat Privada (a partir d'ara LSP), constitueix el nou marc jurídic de la videovigilància en l'àmbit privat, derogant l'anterior Llei 23/1992, de 30 de Juliol, així com la norma reglamentària que la desenvolupava, el Reial Decret 2364/1994, en tot allò que se li oposi.

La LSP reconeix, en el Preàmbul, la importància de la seguretat privada en la seva labor complementària de la seguretat pública, i es refereix a que “resulta especialment rellevant la regulació dels serveis de videovigilància i d'investigació privada, ja que es tracta de serveis que potencialment poden incidir de forma directa en l'esfera de la intimitat dels ciutadans”.

La nova LSP regula en un article específic, concretament l'art. 42, els serveis de videovigilància de les empreses de seguretat privada. És el mateix art. 42 en el seu primer punt on es defineix el servei de videovigilància. No obstant, apareix una novetat a partir de la qual s'estableix una diferència en funció de la finalitat de tal servei, segons la qual el servei haurà de ser prestat de manera necessària per un vigilant de seguretat o per personal diferent al de seguretat privada. Així doncs, quan la finalitat sigui la seguretat, entesa com el control de l'accés autoritzat i la prevenció de danys i infraccions, únicament podrà ser realitzat per personal de seguretat, mantenint lliure la prestació pels casos de comprovació d'instal·lacions, accessos a aparcament i les activitats de control d'autopistes de peatge (ARITIO, 2004). No obstant l'anterior, hi ha finalitats que no han sigut recollides i sobre les que el precitat art. 42 guarda silenci, com és l'ús de la videovigilància per al control laboral. Hem de pensar, d'aquesta manera, que també queden fora, és a dir, el seu règim és idèntic als que estan exclosos, com el control a accessos a aparcaments i garatges? (SEMPERE, 2014).

També, en l'art. 5.1.f) de la LSP s'assenyala que constitueixen activitats de seguretat privada la instal·lació i manteniment d'aparells, equips, dispositius i sistemes de seguretat connectats a centrals receptores d'alarmes o a centres de control o de videovigilància. D'altra banda, queden fora de l'àmbit d'aplicació de la LSP, segons estableix el seu art. 6.1.b), la fabricació, comercialització, venda o entrega d'equips tècnics de seguretat electrònica, així com la instal·lació o manteniment de tals equips sempre que no estiguin connectats a centrals d'alarma o centre de control o de videovigilància. És a dir, la nota essencial per considerar l'aplicació de la LSP a la instal·lació de sistemes de videovigilància és que aquests estiguin connectats a una central d'alarmes (ÁLVAREZ, 2014, p. 14-15).

Partint de la base del que s'ha mencionat anteriorment, es necessari distingir dos tipus de videovigilància en l'àmbit laboral, la que es produeix en circuit obert o tancat. En el primer cas, el sistema de captació i/o gravació d'imatges està connectat a una central d'alarmes d'una empresa privada de seguretat, l'àmbit del qual està ordenat per la LSP. En el segon cas, és el propi empresari qui instal·la, grava i controla les gravacions sota la seva iniciativa i responsabilitat. No existeix encara norma alguna que reguli la videovigilància efectuada pel propi empresari, posant de relleu l'existència d'una llacuna legal en aquest àmbit.

L'apartat 42.2 LSP prohibeix la instal·lació i gravació d'imatges ni sons de la via pública, excepte d'aquella realitzada per les Forces i Cossos de Seguretat. En aquest sentit, el mencionat article obre el camí a l'ús de la seguretat privada en espais, vies i llocs d'accés públics, "sempre i quan ho permeti la normativa específica i existeixi autorització administrativa" (SEMPERE, 2014). La pròpia LSP justifica tal oportunitat ja que "també s'ha aprofitat per a realitzar una necessària matisació del principi general d'exclusió de la seguretat privada dels espais públics, la formulació actual de la qual avui resulta obsoleta, ja que degut a la seva excessiva rigidesa ha dificultat o impedit la necessària autorització de serveis en benefici del ciutadà" (Preàmbul V LSP). Al respecte, també es pronuncia l'art. 4.3 de la Instrucció 1/2006, segons el qual les videocàmeres instal·lades en espais privats no podran obtenir imatges dels espais públics, excepte que resulti imprescindible per la finalitat de vigilància que es pretén assolir, o resulti impossible evitar-ho per raó de la ubicació d'aquestes.

La videovigilància privada troba aplicacions com ara:

“La seguretat privada en la llar, en qualsevol transport privat i qualsevol establiment privat, en els fins de control laboral i de producció per assegurar el degut acompliment dels treballadors, en centres educatius i guarderies, entre d’altres” (IBARRA, 2011, p. 258).

1.3 Finalitats

La captació i/o tractament d’imatges generalment persegueix garantir la seguretat dels béns i les persones o s’utilitza en entorns empresarials amb la finalitat de verificar el compliment per part del treballador de les seves obligacions i deures laborals (INTECO, 2011, p. 4). Així doncs, la protecció de les persones, la protecció de la propietat, l’interès públic, la detecció, prevenció i càstig de delictes i altres interessos legítims constitueixen la base dels arguments que justifiquen la instal·lació de sistemes de videovigilància (ABA, 2003, p. 14).

1.3.1 Seguretat

La seguretat és el principal motiu pel qual es realitza, amb major freqüència, la instal·lació de sistemes de videovigilància. De forma general suposa l’ús de la videovigilància amb fins de seguretat dels béns materials i de les persones. Aquesta finalitat inclou la captació d’imatges per controlar la seguretat ciutadana, la seguretat vial, els esdeveniments esportius, l’accés a entorns privats, etc. (INTECO, 2011, p. 4).

El seu principal objectiu és mantenir l’ordre públic, protegir la integritat física de les persones, així com dels béns, prevenir la comissió de delictes i infraccions administratives, col·laborar en la investigació i persecució de delictes, auxiliar a la població en cas de sinistres i desastres, aportar elements probatoris en el desenvolupament d’algun procés jurisdiccional, entre d’altres (IBARRA, 2011, p. 243).

1.3.2 Control empresarial

Implica l’ús de la videovigilància en entorns empresarials amb fins de control laboral, en virtut de l’exercici de la potestat de vigilància del compliment de la relació laboral

que l'art. 20.3 del Reial Decret Legislatiu 2/2015, de 23 d'Octubre, pel que s'aprova el text refós de l'Estatut dels Treballadors (a partir d'ara ET) atorga als empresaris. En aquest cas, la utilització de les càmeres es destina a proporcionar informació a l'empresari sobre el compliment per part del treballador de les seves obligacions i deures laborals (INTECO, 2011, p. 4). En molts casos, la vigilància per videocàmera ve justificada per la detecció i la verificació de conductes il·lícites o la prevenció de delictes per part del treballador o de tercers (usuaris, clients, etc.). Però la utilització dels mitjans audiovisuals en l'interior de l'empresa no pot ser emmarcada només en el context de la seguretat i la protecció de les persones i dels béns. Es relaciona, també, amb altres interessos; és una excel·lent eina de control de l'activitat laboral dels treballadors, una nova forma de governar les relacions laborals, substancialment basada en el coneixement i flux d'informació que proporciona. Aquesta facultat de verificació té els seus límits i no pot realitzar-se de manera que atempti contra el dret a la intimitat dels treballadors (GOÑI, 2007, p.16).

La utilització d'aquest instrument de control ofereix notables avantatges sobre l'acció de vigilància directa que en el passat s'exercia a través del personal específic encarregat de tasques de vigilància. En primer lloc, la videovigilància multiplica la capacitat de vigilància, ja que supera l'àrea de percepció visual del personal de vigilància, permetent així un control més intens, universal i generalitzat. També permet exercir una vigilància sobre “aspectes de l'activitat diària dels treballadors que no influeixen en el comportament per la realització del treball i en la obtenció de resultats” (GOÑI, 2007, p. 17). A la vegada, la solució de la videovigilància suposa un estalvi de costos important per l'empresa, ja que l'ús d'aquest mecanisme de control resulta molt més econòmic que la supervisió humana. Entre els múltiples avantatges que proporciona la videovigilància a l'àmbit laboral, tampoc pot ignorar-se l'efecte psicològic que causa. D'una banda, es tracta d'una important eina dissuasòria de prevenció d'il·lícits laborals, i de l'altra, resulta un instrument eficaç per assegurar el comportament diligent del treballador (GOÑI, 2007, p. 17-18).

Aquests sorprenents nivells d'inspecció empresarial, assolits amb aquests nous dispositius tecnològics, plantegen, no obstant, importants problemes ètico-jurídics al posar en perill, no només la llibertat i la dignitat dels treballadors observats, sinó també el seu propi equilibri psíquic, i elevar el poder empresarial al grau “d'omnipotent, anònim i invisible” (GUDE, 2014, p. 46). S'ha demostrat en investigacions empíriques

que la videovigilància en el lloc de treball causa alguns efectes negatius. Segons aquestes, els treballadors que són objecte de monitorització tenen més probabilitats de sentir desconfiança, desmotivació, amb menys sentiments de lleialtat i un major estrés (GUDE, 2014, p. 46).

1.3.3 Altres fins

L'auge d'aquest tipus de sistemes ha afavorit el seu ús en altres àmbits molt variats, tals com la promoció turística, la investigació, els estudis conductuals, etc. Per exemple, cada vegada és més comú la instal·lació de sistemes de videovigilància per a la promoció de diversos llocs, mitjançant la visualització online a través d'Internet, com poden ser determinades gravacions de parts d'una ciutat ofertes des de la pàgina web d'un ajuntament. També s'està donant la utilització de sistemes de videogravació en el que respecta a informació relativa a persones, ja sigui per investigació científica o per la realització d'estudis d'hàbits d'ús o consum, o els relacionats amb el desenvolupament de la tecnologia de videogravació (INTECO, 2011, p. 4).

2. Videovigilància i Drets Fonamentals

Els drets fonamentals potencialment afectats per la utilització de la videovigilància són nombrosos. Aquests es poden classificar en dos grups: d'una banda, hi ha els drets relatius a la protecció de la vida privada, i de l'altra, els drets de llibertat. En el catàleg de drets fonamentals que podrien veure's afectats, s'hi poden incloure: la llibertat ideològica (art. 16 CE), el dret a la intimitat personal (art. 18.1), el dret a la pròpia imatge (art. 18.1 CE), la inviolabilitat del domicili (art. 18.2 CE), el secret de les comunicacions (art. 18.3 CE), la protecció davant el tractament automatitzat de dades de caràcter personal (art. 18.4 CE), la llibertat de circulació (art. 19 CE), el dret de reunió i de manifestació (art. 21 CE), el dret a la tutela judicial efectiva (art. 24.1 CE) i la llibertat sindical i el dret de vaga (art. 28 CE) (ARZOZ, 2002, p. 140).

Els drets a la intimitat i a la pròpia imatge són els que semblen afectats de forma més general i directa, ja que els sistemes de videovigilància tenen precisament la finalitat de la captació, i en el seu cas la gravació, d'imatges i sons de les persones que transiten per aquells llocs on les videocàmeres estan situades. En altres casos, el supòsit de fet de l'afectació del dret requereix d'un element addicional, com ara el lloc d'emplaçament de les videocàmeres. Aquest és el cas del dret a la inviolabilitat del domicili. Per últim, el supòsit de fet d'afectació d'alguns drets (llibertat ideològica, dret de reunió, llibertat sindical, etc.) és més complex, ja que requereix la concurrència de múltiples elements (ETXEBERRIA ET AL., 2011, p. 158-159).

2.1 Dret a la intimitat personal

2.1.1 Concepte i evolució

És el dret fonamental més directa i intensament implicat per la tecnologia de la videovigilància. El dret a la intimitat està reconegut a l'art. 18.1 CE, i ha de ser entès, d'acord amb l'art. 10.2 CE, com a dret al respecte de la vida privada; és a dir, segons la interpretació efectuada pel Tribunal Europeu de Drets Humans (a partir d'ara TEDH), com el dret al respecte d'un àmbit en el que l'individu pugui perseguir lliurement el desenvolupament de la seva personalitat (ARZOZ, 2002, p. 143). No obstant, no apareix definit ni en la CE ni en la LO 1/1982, de 5 de Maig, de protecció civil del dret a

l'honor, a la intimitat personal i familiar i a la pròpia imatge (a partir d'ara LOPH), constituint així un concepte jurídic indeterminat. La citada LOPH estableix, en el seu art. 2.1, dos elements que permeten la seva delimitació i configuració: un de caràcter objectiu, que ve establert per les lleis i usos socials i, un de caràcter subjectiu, que és l'àmbit que, pels seus propis actes, mantingui cada persona reservat per sí a mateix o per a la seva família (SEGOVIANO, 2004, p. 154).

Aquest precepte posa de relleu que el concepte d'intimitat no és igual per a totes les persones, sinó que s'ha de tenir en compte si es tracta de persones que exerceixen un càrrec públic o una professió de notorietat o projecció pública (art. 8 LOPH). L'art. 7 tipifica les intromissions il·legítimes en aquest dret. Algunes de les conductes considerades com a constitutives d'intromissió il·legítima són l'al·lusió a la vida íntima, a manifestacions o cartes privades, a escrits personals de caràcter íntim i imatges d'una persona en llocs o moments de la seva vida privada, entre d'altres, per la qual cosa el concepte d'intimitat es refereix a un àmbit personal reservat que abraça les activitats del cercle íntim, personal i familiar, excepte per consentiment de l'interessat (SEGOVIANO, 2004, p. 154-155).

Inicialment, la jurisprudència del TC estava caracteritzada per un plantejament confús sobre el contingut del dret a la intimitat, i dominada per una comprensió bastant estreta (negativa o especial) de la intimitat com a àmbit reservat. En efecte, la intimitat era definida recurrentment com “un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario –según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana” (STC 231/1988 i 57/1994). El dret protegiria el ciutadà front les intromissions que per qualsevol mitjà poguessin realitzar-se en tal àmbit reservat de vida (STC 110/1984). No obstant, la idea “d'àmbit reservat” era ambigua ja que determinava una delimitació espacial de l'àmbit protegit (ARZOZ, 2002, p. 141).

La STC 119/2001 va afirmar per primera vegada que el dret a la intimitat, com el dret fonamental a la integritat física i moral i a la inviolabilitat del domicili, són:

“Derechos que han adquirido también una dimensión positiva en relación con el libre desarrollo de la personalidad, orientada a la plena efectividad de estos derechos fundamentales. En efecto, habida cuenta de que nuestro texto constitucional no consagra derechos meramente teóricos o ilusorios, sino reales y efectivos se hace imprescindible asegurar su protección no sólo frente a

las injerencias ya mencionadas, sino también frente a los riesgos que puedan surgir en una sociedad tecnológicamente avanzada (FJ. 5º)”(ARZOZ, 2002, p. 142).

La mateixa sentència estableix que l'objecte del dret a la intimitat “fa referència a un àmbit de la vida de les persones exclòs tant del coneixement aliè com de les intromissions de tercers, i que la delimitació d'aquest àmbit ha de fer-se en funció del lliure desenvolupament de la personalitat”. En suma, la clàusula del “lliure desenvolupament de la personalitat” ha esdevingut el criteri d'interpretació del contingut dels drets de l'art. 18, així com el criteri decisiu per a la determinació de l'existència d'una ingerència en el dret fonamental (ETXEBERRIA ET AL., 2011, p. 160).

Ni el TC ni el TEDH limiten el dret a la intimitat personal a l'àmbit domèstic o privat, sinó que consideren que també desplega la seva eficàcia en l'àmbit públic (ETXEBERRIA ET AL., 2011, p. 161). Al respecte, la sentència *Peck* va ser el primer cas sobre la conformitat de la videovigilància abordat pel TEDH. El Tribunal va entendre que un circuit tancat de televisió en un lloc públic que no grava imatges no constituïa *prima facie* una intromissió a la vida privada. Per al Tribunal, en un àmbit públic qualsevol persona ha d'assumir la possibilitat de ser vista per altres. No obstant, la valoració jurídica es modifica quan les càmeres no es limiten a veure, sinó que també graven les imatges de forma permanent. El que decanta el raonament del TEDH en l'apreciació d'una intromissió és el registre sistemàtic de les imatges, fonamentat en les enormes possibilitats que obre aquest mecanisme. Aquest salt qualitatiu serà el que desencadena la protecció prevista en l'art. 8 del Conveni Europeu de Drets Humans (a partir d'ara CEDH) (ETXEBERRIA ET AL., 2011, p. 162-164).

A la llum de la jurisprudència del TEDH, sembla indubtable que la utilització de videocàmeres que enregistren les imatges en espais públics constitueix una ingerència en el dret al respecte de la vida privada, encara que en principi pugui ser justificable quan respon a una finalitat de seguretat preventiva en una societat democràtica (ETXEBERRIA ET AL., 2011, p. 166).

El concepte clàssic d'intimitat en l'actualitat es troba superat per l'aparició d'una nova situació que emergeix fruit de les noves tecnologies. El desenvolupament informàtic suposa l'aparició d'importants perills per a la intimitat dels ciutadans, degut a que permet el coneixement, emmagatzematge i tractament d'infinat de dades de les persones, facilitant així el coneixement de comportaments, aficions, creences religioses,

etc., de cada individu. Per tant, aquest continu avenç i desenvolupament representa un perill per a la intimitat, excedint per sobre de les seves formes clàssiques de protecció jurídica (SEGOVIANO, 2004, p. 156).

Tal i com va assenyalar el TC en la STC 110/1984, sobre el dret a la intimitat:

“Su idea originaria era el respeto a la vida privada... Lo ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas han obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida” (STC 110/1984, FJ. 3º) (ARZOS, 2002, p.141).

Apareix així, un nou concepte d'intimitat, més ampli i més desenvolupat, el qual resulta definit per Romero Casabona com “aquelles manifestacions de la personalitat individual o familiar, el coneixement o desenvolupament de les quals queden reservats al seu titular o sobre els que exerceix alguna forma de control quan es veuen implicades terceres persones” (SEGOVIANO, 2004, p. 156).

En resum, la videovigilància suposa una ingerència en la doble dimensió de la intimitat, com a àmbit privat reservat davant l'acció i el coneixement dels altres. No es tracta només de la possibilitat d'extreure informació que només pertany a l'esfera privada de les persones (dimensió negativa de la intimitat), sinó també d'una acció que intervé en l'àmbit propi i reservat de les persones i que afecta a la dimensió positiva de la intimitat personal lligada amb el lliure desenvolupament de la personalitat (ETXEBERRIA ET AL., 2011, p. 167).

2.1.2 Dret a la intimitat en l'àmbit laboral

El concepte d'intimitat també es projecta sobre les relacions laborals, tan individuals com col·lectives (SEGOVIANO, 2004, p. 157). Ens trobem davant un concepte jurídic tan ampli com indeterminat, corresponent a la jurisprudència establir el seu àmbit de protecció, atenent particularment a les circumstàncies (personals i objectives) de cada cas en concret. La conceptualització de la intimitat, tal i com ha assenyalat el TC, és oberta i evolutiva en funció del tema específic que s'està tractant (STC 110/1984, FJ 3º) (GUDE, 2015, p. 8-9).

L'art. 4.2.e) de l'ET reconeix el dret a la intimitat davant l'empresari, existint un tractament legal del mateix respecte a registres i controls empresarials en els arts. 18, en el que es reconeix la inviolabilitat de la persona del treballador i 20.3 ET en el que es regula el control de l'activitat laboral. En el contracte de treball aquest dret ha vingut operant com a límit en les ingerències empresarials, així com a com a dret negatiu d'immunitat (GUDE, 2015, p. 7).

La doctrina jurídica l'ha configurat com un dret vinculat a la pròpia personalitat i derivat de la dignitat de la persona reconegut a l'art. 10.1 CE. Preserva a l'individu no només de l'obtenció il·legítima de dades de la seva esfera íntima per part de terceres persones, sinó també de la revelació, divulgació o publicitat no consentida d'aquestes dades, i de l'ús o explotació de les mateixes sense autorització del titular, garantint, per tant, el secret sobre la pròpia esfera de vida personal i, consegüentment, vetant als terceres, particulars o poders públics, decidir sobre els contorns de la vida privada (SSTC 83/2002, FJ 5º i 70/2009, FJ 2º) (GUDE, 2015, p. 7).

Per això, l'empresari no queda apoderat, a l'empara de les facultats de vigilància i control que li confereix l'art. 20.3 ET, per realitzar intromissions il·legítimes en la intimitat dels seus treballadors, sinó que es precís que ponderi aquest dret del treballador junt amb el poder de direcció i control de l'empresari: “los equilibrios y limitaciones recíprocos que se derivan para ambas partes del contrato de trabajo, suponen, que también las facultades organizativas empresariales se encuentren limitadas por los derechos fundamentales del trabajador, quedando obligado el empleador a respetar aquéllos” (STC 292/1993, FJ 4º) (GUDE, 2015, p. 7).

No s'ha d'oblidar que no es tracta d'un dret absolut, sinó que, tal i com ha manifestat el TC, pot cedir davant interessos constitucionalment rellevants sempre i quan la retallada que experimenti “se revele como necesaria para lograr el fin legítimo previsto, proporcionado para alcanzar-lo y, en todo caso, respetuoso con el contenido esencial” (STC 143/1994, FJ 6º). L'esfera de la intimitat personal està directament vinculada amb la delimitació que en faci el titular de la mateixa, havent reiterat l'Alt Tribunal que cada persona pot reservar-se un espai protegit de la curiositat i coneixement aliè, que a cadascú li correspon acotar (STC 159/2009, FJ 3º) (GUDE, 2015, p. 8).

Dins l'àmbit empresarial, els nous mitjans tècnics derivats dels avenços tecnològics han incrementat el poder de l'empresari, el qual pot constituir una amenaça real sobre els

drets del treballador. Els òrgans judicials han convertit la intimitat, per aquesta via, en un límit directe i efectiu a la utilització de les noves tecnologies en el marc de les relacions laborals. El ràpid creixement de les formes de vigilància i control laboral, sustentades en les tecnologies de la informació i comunicació, junt amb l'escassetat de normativa en aquesta matèria, ha encarregat als òrgans judicials l'establiment de les pautes per a l'adequació de tals mitjans de control als drets fonamentals dels treballadors (GUDE, 2015, p. 9).

En un primer moment, la jurisprudència laboral permetia sense cap dubte la instal·lació de videocàmeres per controlar el compliment per part del treballador de les seves obligacions i deures laborals. En els pronunciaments, els tribunals afirmaven que el centre de treball era un lloc públic en el que el treballador no tenia dret a la intimitat i en el que, en conseqüència, la instal·lació d'aquestes sistemes no plantejava cap problema (GUDE, 2015, p. 11). En aquest sentit es va pronunciar el Tribunal Superior de Justícia (a partir d'ara TSJ) de Galícia, en la seva sentència dictada el 25 de gener de 1996:

“La utilización de cámaras para la filmación de la actividad de los trabajadores, ya sea en la recepción, en el bar, en el restaurante o en la cocina del hotel, no puede suponer una invasión de su intimidad ni una lesión de su derecho a la intimidad, pues de entenderlo así, supondría extender la protección de tales derechos a instalaciones que suponen la práctica totalidad de espacios públicos del hotel en el que éste presta sus servicios, y en consecuencia en donde los trabajadores desarrollan su actividad” (FJ 3º).

Inicialment, el desenvolupament de l'activitat laboral en el lloc de treball no estava emparada pel dret a la intimitat, ja que el referit dret s'exercita en l'àmbit de l'esfera privada del treballador, que en l'empresa s'ha d'entendre limitat als llocs de descans, vestuaris, serveis i altres similars, però no en aquells llocs en que es desenvolupa l'activitat laboral. En la mateixa línia es situava un sector de la doctrina científica, que avalava l'ús de videocàmeres en l'àmbit laboral per entendre que no vulnerava el dret a la privacitat dels treballadors (GUDE, 2015, p. 12).

En conseqüència, tant la jurisprudència com la doctrina jurídica:

“Negaven l'existència d'un conflicte quan s'instal·laven càmeres de seguretat en les empreses amb el dret dels treballadors a protegir la seva intimitat, al no reconèixer-se'ls quan estaven executant la prestació de serveis en el temps i lloc de treball. L'activitat laboral no era un acte íntim sinó social que, d'aquesta forma, podia ser supervisat sempre i quan la inspecció es mantingués dins dels límits estrictament contractuals” (GUDE, 2015, p. 12).

L'any 2000 el TC va dictar dos importants sentències en la matèria que van suposar un important canvi en la doctrina jurisprudencial: van ser la STC 98/2000, de 10 d'Abril i la STC 186/2000, de 10 de Juliol. En resum, ambdós sentències neguen la premissa mantinguda per la jurisprudència fins al moment, la de que en el centre de treball no pot constituir, per definició, un espai en el que exercir el dret a la intimitat dels treballadors. La intimitat, tal i com afirmen aquestes decisions judicials, existeix també en el lloc de treball i ha de ser protegida davant possibles intromissions de l'empresari (GUDE, 2015, p. 14).

El criteri jurisprudencial inicial, basat en la consideració del centre de treball com un àmbit apart a la intimitat, ha sigut desplaçat per aquests pronunciaments per la tècnica de la ponderació. A partir d'ara, els tribunals analitzaran cada cas plantejat en concret, i sotmetran la videovigilància al criteri de la proporcionalitat. Per valorar si el sistema de videovigilància constitueix una intromissió il·legítima sobre el dret a la intimitat del treballador, els tribunals prendran en consideració diferents aspectes:

“Si la col·locació de les càmeres es fa o no de forma indiscriminada i massivament, si els sistemes són visibles o han sigut instal·lats subreptíciament, quina és la finalitat perseguida amb el seu emplaçament, si existeixen raons de seguretat suficient tenint en compte l'activitat que es desenvolupa en el centre de treball per implantar mitjans de control amb càmeres, etc” (GUDE, 2015, p. 15).

No obstant, tal i com apunten Desdentado Bonete i Muñoz Ruiz, potser també resulta excessiu entendre que la presència de càmeres en el lloc de treball provoca sempre, i en qualsevol circumstància, una vulneració del dret a la intimitat (DESDENTADO & MUÑOZ, 2012, p. 25) (GUDE, 2015, p. 15).

2.2 Dret a la pròpia imatge

Un altre dret fonamental potencialment afectat per la videovigilància és el dret a la pròpia imatge. La protecció constitucional que gaudeix la pròpia imatge pot estar directament relacionada amb l'àmbit de la intimitat personal i familiar, com suggereix el context de l'art. 18.1 CE, però no és plenament coincident (ARZOZ, 2002, p.146). Moltes han sigut les dificultats existents per perfilar el concepte d'aquest dret respecte del dret a l'honor, i especialment, a la intimitat (CHAPARRO & TALENS, 2012, p. 255).

No obstant, l'autonomia conceptual del dret es troba actualment superada gràcies al pronunciament exprés del TC. Aquest és un dret autònom respecte del dret a la intimitat o a l'honor, i la STC 81/2011 identifica l'objecte del dret amb els "trets físics personals", això és "l'aspecte físic". Aquesta sentència, transcendental per l'àmbit de protecció del dret a la pròpia imatge, considera sobre el contingut del dret fonamental (ETXEBERRIA ET AL., 2011, p. 168-169):

"La facultad otorgada por este derecho, en tanto que derecho fundamental, consiste en esencia en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad -informativa, comercial, científica, cultural, etc.- perseguida por quien la capta o difunde" (FJ 2º).

El TC diferencia els àmbits que protegeixen cadascun dels citats drets, afirmant que "allò específic del dret a la pròpia imatge és la protecció front a les reproduccions de la mateixa, que afectant a l'esfera personal, no lesionen el seu bon nom ni donen a conèixer la seva vida íntima. El dret a la pròpia imatge pretén salvaguardar un àmbit propi i reservat, però no íntim" (CHAPARRO & TALENS, 2012, p. 256).

L'afirmació constitucional d'un dret fonamental a la pròpia imatge es realitza amb plena desvinculació del lloc públic o privat (ETXEBERRIA ET AL., 2011, p.169).

El TC ha establert que:

"El derecho a la propia imagen, reconocido por el art. 18.1 de la Constitución al par de los del honor y la intimidad personal, forma parte de los derechos de la personalidad y como tal garantiza el ámbito de libertad de una persona respecto de sus atributos más característicos, propios e inmediatos como son la imagen física, la voz o el nombre, cualidades definitorias del ser propio y atribuidas como posesión inherente e irreductible a toda persona. En la medida en que la libertad de ésta se manifiesta en el mundo físico por medio de la actuación de su cuerpo y las cualidades del mismo, es evidente que con la protección de la imagen se salvaguarda el ámbito de la intimidad y, al tiempo, el poder de decisión sobre los fines a los que hayan de aplicarse las manifestaciones de la persona a través de su imagen, su identidad o su voz" (STC 117/1994, FJ. 3º).

En suma, el dret a la pròpia imatge i a la pròpia veu atorga al titular el poder de disposició d'aquests béns jurídics davant les possibles utilitzacions de tercers. D'aquesta manera, la videovigilància constitueix una ingerència en el dret a la pròpia imatge ja que les imatges i/o veus són captades, gravades i utilitzades, ja sigui per les Forces i Cossos

de Seguretat o pels subjectes responsables dels sistemes privats de videovigilància, sense el consentiment dels seus titulars (ARZOZ, 2002, p. 148).

En suma, la videovigilància, en la mesura que es capti la imatge i la veu de les persones sense el seu consentiment, amb independència del caràcter íntim o reservat del moment o circumstància, estarà afectant el dret a la pròpia imatge.

2.2.1 El dret a la pròpia imatge en l'àmbit laboral

El dret a la pròpia imatge en la vessant laboral està marcat per l'especial relació de subordinació que ostenta el treballador davant l'empresari, la qual cosa justifica que, en determinades ocasions, hagi de prevaldre el dret a la llibertat d'empresa. No obstant, s'ha de partir de la base de que el treballador manté els drets inherents a la persona (CHAPARRO & TALENS, 2012, p. 257).

En l'àmbit laboral es clàssica la distinció entre aquells drets fonamentals específics de la pròpia relació laboral, com per exemple el dret a la llibertat sindical (art. 28.1 CE) o el dret de vaga (art. 28.2 CE), d'aquells denominats inespecífics, és a dir, els que no són pròpiament laborals però poden exercitar-se en el sí de la relació de treball. El dret a la pròpia imatge és, per tant, un dret inespecífic, i manca d'una regulació específica en l'àmbit laboral (CHAPARRO & TALENS, 2012, p. 258).

Per protegir aquest dret, és freqüent recórrer a l'art. 4.2.e) ET, que incideix en aquest aspecte al disposar que en la relació de treball els treballadors tenen dret al respecte de la seva intimitat i a la consideració deguda de la seva dignitat. De la mateixa manera, l'art. 8.11 del Reial Decret Legislatiu 5/2000, de 4 d'Agost, pel que s'aprova el text refós de la Llei d'Infraccions i Sancions en l'Ordre Social (a partir d'ara LISOS), qualifica com a infracció molt greu “els actes de l'empresari que siguin contraris al respecte de la intimitat i consideració deguda a la dignitat dels treballadors” (CHAPARRO & TALENS, 2012, p. 258).

2.3 Dret a la protecció de dades

El dret a la protecció de dades ha sigut regulat en el dret espanyol a l'art. 18.4 CE, com un mandat al legislador per a que limiti l'ús de la informàtica per garantir l'honor i la intimitat personal i familiar dels ciutadans, i el ple exercici dels seus drets (GUDE, 2014, p. 51).

En un primer moment, la LO 5/1992, de 29 d'Octubre, de Regulació de Tractament Automatitzat de Dades de Caràcter Personal (a partir d'ara LORTAD), i després la LOPD, es van encarregar d'afrontar la seva tutela. Ambdós normes es van inspirar en legislació europea: la LORTAD es va inspirar en el Conveni 108 del Consell d'Europa, de 28 de Gener de 1981, per a la tutela de les persones en relació amb el tractament automatitzat de dades de caràcter personal; i la LOPD en la Directiva 95/46/CE del Parlament Europeu, de 24 d'Octubre de 1995, relativa a la protecció de les persones físiques en el que respecta al tractament de dades personals i la seva lliure circulació (GUDE, 2014, p.51-52). No obstant, actualment la Directiva 95/46/CE ha estat derogada pel recent Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'Abril de 2016.

A més, el TC també s'ha encarregat de la construcció del dret a la autodeterminació informativa en un grup de sentències, principalment la STC 254/1993, de 20 de Juliol i la STC 292/2000, de 30 de Novembre.

Per al TC, l'art. 18.4 CE incorpora una nova garantia constitucional, com a resposta a una nova forma d'amenaça concreta a la dignitat i als drets de la persona. La garantia reconeguda a l'art. 18.4 CE constitueix un dret fonamental amb una doble dimensió, una instrumental i una altra autònoma. D'una banda, representa un “instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad” (STC 254/1993, FJ. 6º). De l'altra, “consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona... pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos propicie comportamientos discriminatorios” (STC 11/1998, FJ. 5º) (ARZOZ, 2002, p. 149).

El dret a la protecció de dades s'orienta a garantir al seu titular el control sobre les dades personals i el seu ús i destí, amb el propòsit d'impedir el seu tràfic il·lícit i lesiu per a la

dignitat i drets del afectat. Per tant, davant el dret a la intimitat que reconeix “el poder de resguardar la vida privada de una publicidad no querida, el derecho a la protección de datos garantiza el poder de disposición sobre los mismos” (STC 292/2000, FJ. 6º) (GUDE, 2014, p. 53). Pel que fa al seu objecte, per a l’Alt Tribunal el dret a l’autodeterminació informativa no es redueix només a les dades íntimes de la persona, sinó a qualsevol tipus de dada personal, el coneixement o ús de la qual per tercers pugui afectar als seus drets, siguin o no fonamentals. També abraça a aquelles dades personals públiques que, pel fet de ser-ho, de ser accessibles al coneixement de qualsevol persona, no escapen del poder de disposició de l’afectat. Per últim, el dret a la protecció de dades comprèn diversos poders el qual exercici imposa a tercer deures jurídics: el dret a que es requereixi el consentiment previ per a la recollida i ús de les dades personals, a ser informat sobre el destí i ús d’aquelles dades i a accedir, rectificar i cancel·lar tals dades.

Les relacions de la videovigilància amb el dret fonamental a la protecció de dades de caràcter personal són complexes a la llum de la legislació vigent (ETXEBERRIA ET AL., 2011, p. 172). Les videocàmeres reproduïxen imatges dels afectats i, a efectes de la LOPD, la imatge d’una persona constitueix una dada de caràcter personal. Per tant, la informació obtinguda a través dels sistemes de videovigilància es troba sotmesa a la LOPD, en la mesura que sigui objecte d’un tractament manual o automatitzat. En aquells casos que no s’enregistren ni es conserven imatges, sinó que es limiten a reproduir-les, la Instrucció 1/2006 preveu que no serà necessari inscriure fitxer quan el tractament consisteixi exclusivament en la reproducció o emissió d’imatges en temps real (DESDENTADO & MUÑOZ, 2012, p. 63).

La intromissió consisteix en la gravació de les imatges i en la seva conservació i, per tant, en la disponibilitat durant un temps rellevant. Així doncs:

“Si el dispositiu capta imatges que identifiquen o permeten identificar persones, però les imatges no es graven, ni es transmeten, ni són objecte de tractament o aplicació, és cert que es recullen dades personals i que aquestes passen a coneixement de qui observa, però degut a la seva volatilitat, i les limitades possibilitats d’una utilització posterior de la informació, sembla existir un perill relativament menor per al bé jurídic protegit” (ETXEBERRIA ET AL., 2011, p. 173-174).

2.3.1 El dret a la protecció de dades en l'àmbit laboral

Segons l'art. 4 LOPD, seguint l'art. 5 del Reglament (UE) 2016/679, les dades de caràcter personal només es podran recollir per al seu tractament quan siguin “adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per les que s'hagin obtingut”. En l'àmbit de la videovigilància laboral, la legitimitat ve donada per les facultats de control empresarial que reconeix l'art. 20.3 ET, sempre i quan no siguin abusives (DESDENTADO & MUÑOZ, 2012, p. 63).

Són elements característics de la definició constitucional del dret fonamental a la protecció de dades personals “los derechos del afectado a que se requiera el previo consentimiento para la recogida y uso de los datos personales, a ser informado sobre el destino y uso de esos datos y a acceder, rectificar y cancelar dichos” (STC 292/2000, FJ 7º).

El consentiment de l'afectat és, per tant, l'element definidor del sistema de protecció de les dades de caràcter personal. D'aquesta manera, l'art. 6.1 LOPD preveu que el tractament de dades de caràcter personal requerirà el consentiment inequívoc de l'afectat, excepte que la llei disposi una altra cosa. El núm. 2 del mateix precepte conté una llarga llista de supòsits en els que el consentiment no es necessari. Un d'ells dispensa tal consentiment “quan el tractament de les dades es refereixi a les parts d'un contracte o precontracte d'una relació comercial, laboral o administrativa i sigui necessari per al seu manteniment i compliment” (DESDENTADO & MUÑOZ, 2012, p. 65).

En l'àmbit laboral el consentiment passa, per tant, com a regla general a un segon pla. Es presumeix que el consentiment donat pel treballador per la formalització del vincle jurídic contractual permet també la recollida i tractament de dades, la qual cosa possibilita la captació de les imatges sense necessitat de cap altre pronunciament exprés (GUDE, 2014, p. 57-58). Aquesta excepció a l'exigència de consentiment apareix també recollida a l'art. 10.3.b) RLOPD.

En conseqüència, el règim de protecció de dades aplicat a la videovigilància en l'àmbit laboral, no requereix el consentiment exprés del treballador per instal·lar càmeres a l'empresa o procedir al tractament d'imatges obtingudes amb finalitats de control laboral, això és les obligacions derivades del contracte de treball. Malgrat això, sí es

precisarà el consentiment de l'afectat quan el tractament de les dades tingui altres objectius o destins aliens al contracte de treball (GUDE, 2014, p. 58).

Ara bé, encara que no sigui necessari el consentiment del treballador en els casos assenyalats, el deure d'informació segueix existint, doncs aquest permet a l'afectat exercir els d'accés, rectificació, cancel·lació i oposició. L'art. 3 de la Instrucció 1/2006, de l'AEPD exigeix que els responsables que disposin de sistemes de videovigilància hauran de col·locar distintius informatius en un lloc suficientment visible, així com tenir a disposició impresos en els que es detalli la informació necessària sobre tal mesura (GUDE, 2014, p. 57).

El deure d'informació prèvia forma part del contingut essencial del dret a la protecció de dades, degut a que resulta un complement indispensable de la necessitat de consentiment de l'afectat, ja que si no es coneix la finalitat i destinataris de les dades, difícilment pot prestar-se tal consentiment (DESDENTADO & MUÑOZ, 2012, p. 65).

Si bé el consentiment del treballador no es necessari per a poder gravar la seva imatge, sí és imprescindible que l'empresari informi a aquests de forma expressa i inequívoca dels elements establerts a l'art. 5.1 LOPD (GUDE, 2014, p. 59). No es requereix que la informació es faciliti per escrit. Convé recordar que l'art. 18 RLOPD especifica que aquesta obligació d'informació es durà a terme a través d'un mitjà que permeti acreditar el seu compliment. En ocasions, la informació verbal no queda acreditada, incomplint-se així el que estableix el mencionat precepte (DESDENTADO & MUÑOZ, 2012, p. 67). L'Audiència Nacional (a partir d'ara AN), en la sentència de 15 de Juny de 2001, ha assenyalat sobre aquest deure que “se trata de un derecho de suma importancia ya que es el que permite llevar a cabo el ejercicio de otros derechos”. L'omissió d'aquesta obligació per part dels empresaris ha sigut sancionada en nombroses ocasions per l'AEPD (GUDE, 2014, p.60).

En la recent sentència de 3 de Març de 2016, el Ple del TC ha confirmat la possibilitat de gravar als treballadors sense el seu consentiment previ, sempre que aquest tractament resulti necessari per al compliment del contracte firmat entre les parts, si bé es necessari complir amb el deure d'informació del tractament de dades. En el compliment d'aquest deure d'informació, ja no s'exigeix una informació expressa, precisa, clara i inequívoca de la finalitat de tal control, sinó que la simple col·locació del corresponent cartell

distintiu es suficient per entendre complert el requisit de l'art. 5 LOPD, modificant el criteri que la jurisprudència ja elaborada per aquest Tribunal havia establert.

En el vot particular de la mateixa, els Magistrats Valdés i Asua afirmen que la sentència suposa un “retrocés en la protecció dels drets fonamentals” dels treballadors i entenen que la instal·lació de les càmeres sense informació prèvia expressa, va vulnerar el seu dret fonamental a la pròpia imatge. En la seva opinió, la sentència modifica la doctrina donada fins ara pel Tribunal, oblidant la dimensió del dret a la pròpia imatge protegida per l'art. 18.4 CE. Adverteixen que “les imatges gravades poden servir a propòsits tan inquietants com la confecció d'un perfil ideològic, racial, sexual, econòmic o de qualsevol altra índole, o posar-se al servei d'altres amenaces contra l'individu”. Per últim, consideren que la sentència “confon la legitimitat del fi” perseguit en aquest cas concret per l'empresa (verificar el compliment de les obligacions laborals de la treballadora) amb la “constitucionalitat de l'acte” en sí (que exigeix oferir prèviament la informació necessària sobre la finalitat de la instal·lació de les càmeres). D'altra banda, Xiol afegeix que la informació genèrica sobre la instal·lació de càmeres de videovigilància dirigida al públic és insuficient en l'àmbit laboral.

2.4 Llibertat ideològica, el dret de reunió i manifestació, la llibertat sindical i el dret de vaga

D'acord amb la jurisprudència constitucional, la llibertat ideològica comprèn una dimensió externa i una dimensió interna (ARZOZ, 2002, p. 153):

“La libertad ideológica no se agota en una dimensión interna de derecho a adoptar una determinada posición intelectual ante la vida y a representar o enjuiciar la realidad según personales convicciones. Comprende, además, una dimensión externa de *agere licere*, con arreglo a las propias ideas sin sufrir por ello sanción o demérito ni padecer la compulsión o la injerencia de los poderes públicos” (STC 120/1990, FJ. 10º, 137/1990, FJ. 8º i 141/2000, FJ. 4º).

Per apreciar una vulneració en la llibertat de creences, en la seva dimensió externa, es requereix una interferència suficientment qualificada:

“Ahora bien, para que los actos de los poderes públicos puedan ser anulados por violaciones de la libertad ideológica reconocida en el art. 16.1 CE es cuando menos preciso, de una parte, que aquellos perturben o impidan de algún modo la adopción o el mantenimiento en libertad de una

determinada ideología o pensamiento y no simplemente que se incida en la expresión de determinados criterios. De otra, se exige que entre el contenido y sostenimiento de éstos y lo dispuesto en los actos que se combatan quepa apreciar una relación de causalidad suficiente para articular la imputación del ilícito constitucional” (STC 120/1990, FJ. 10º, 137/1990, FJ. 8º i 141/2000, FJ. 4º).

Aquesta consideració de les dimensió externa de la llibertat ideològica justifica un tractament conjunt amb els drets constitucionals que consagren formes específiques d’expressió i reivindicació de naturalesa col·lectiva: el dret de reunió i manifestació i la llibertat sindical i el dret de vaga (ARZOZ, 2002, p. 154).

La utilització de la tecnologia de la videovigilància sembla no afectar *prima facie* l’exercici dels drets de reunió, llibertat sindical i el dret de vaga o la llibertat ideològica, ja que la instal·lació i utilització de videocàmeres no impedeix ni impossibilita l’exercici de cap dret. No obstant, l’apreciació de l’afectació dels mencionats drets fonamentals per la utilització de videocàmeres no es fonamenta en l’existència d’una col·lisió frontal i directa amb tals drets, sinó que es tracta d’una obstaculització indirecta que redueix la seva efectivitat i plenitud. Aquesta efectivitat pot veure’s reduïda si els propis ciutadans es retracten del seu exercici legítim per temor a les possibles conseqüències negatives que pugui suposar l’enregistrament de la seva participació en reunions o manifestacions (ARZOZ, 2002, p. 154).

El Tribunal Constitucional Federal alemany reflexiona sobre la incidència de les tecnologies informàtiques sobre el lliure exercici dels drets fonamentals:

“Quien sepa de antemano que su participación, por ejemplo, en una reunión o en una iniciativa ciudadana va a ser registrada por las autoridades y que podrán derivarse riesgos para el por este motivo renunciará presumiblemente al ejercicio de los correspondientes derechos fundamentales” (BVerfGE 65, 1 [42 s.]).

Per la seva part, el TC espanyol s’ha pronunciat sobre la utilització de videocàmeres en ocasió al dret de vaga, concretament sobre uns piquets informatius:

“La filmación entrañó una disuasión u obstaculización del libre ejercicio del derecho de huelga, reduciendo su efectividad, pues no cabe minusvalorar los efectos disuasorios que puede producir en el ánimo de quienes pacíficamente forman parte de un piquete informativo el hecho de ser ininterrumpidamente filmados, sin mediar explicación alguna de este proceder. Es más, esos efectos disuasorios pueden enervar los efectos de extensión y publicidad de la huelga por quienes ejercen ese derecho constitucional” (STC 37/1998, FJ. 6º).

Aquest acaba apreciant la incidència efectiva de la videovigilància sobre el mencionat dret, concloent:

“En suma, las circunstancias concurrentes permiten afirmar que la filmación incidió en el ámbito constitucionalmente protegido del derecho de huelga, configurándose como un obstáculo, objetivamente constatable, al modo de lo dicho en la STC 53/1995 (fundamento jurídico 2.º), para la plena efectividad del derecho de huelga”.

En conclusió, la utilització de videocàmeres pot constituir, d'acord amb la naturalesa de les accions objecte d'observació, una ingerència en el dret fonamental a la llibertat ideològica (art. 16.1 CE), en el dret de reunió i de manifestació (art. 21 CE), en la llibertat sindical o en el dret de vaga (art. 28 CE) (ARZOZ, 2002, p. 156).

2.5 Dret al secret de les comunicacions

La Constitució protegeix el dret al secret de les comunicacions en l'art. 18.3 CE (DESDENTADO & MUÑOZ, 2012, p. 190). Mitjançant la videovigilància es poden captar, sens dubte, conversacions directes entre persones. No obstant, la doctrina majoritària considera que el dret fonamental al secret de les comunicacions es refereix a la intervenció de mitjans tècnics de transmissió de missatges entre persones determinades. Això implica que les conversacions directes o en persona queden fora de l'àmbit de protecció de l'art. 18.3 CE (ETXEBERRIA ET AL., 2011, p. 171).

L'objecte de protecció d'aquest dret fonamental és la comunicació, que es concep com “un procés de transmissió de missatges entre persones determinades”, per la qual cosa només es protegeix “l'intercanvi d'objectes a través dels quals es transmeten missatges mitjançant signes lingüístics”, i sempre i quan es tracti d'una comunicació indirecta, és a dir, a distància. Les comunicacions directes no són objecte de protecció per la via de l'art. 18.3 CE, encara que poden ser-ho a través del dret a la intimitat. L'exclusió s'explica en la major vulnerabilitat de la comunicació indirecta (DESDENTADO & MUÑOZ, 2012, p. 190).

En conseqüència, ha de concloure's que la utilització de càmeres de vídeo per a la captació de sons incloses converses no afecta al contingut del dret fonamental al secret de les comunicacions (ETXEBERRIA ET AL., 2011, p. 171).

Malgrat l'anterior, no significa que el contingut de les conversacions directes entre persones quedi desproveït de protecció constitucional. Les escoltes de conversacions directes, ja sigui en llocs oberts o tancats, mitjançant micròfons constituïran una ingerència en el contingut del dret fonamental a la intimitat (ETXEBERRIA ET AL., 2011, p. 171).

2.6 Dret a la inviolabilitat del domicili

La inviolabilitat del domicili pot veure's afectada per la instal·lació de sistemes de videocàmeres, ja que les tecnologies permeten captar les activitats i conductes desenvolupades en l'interior dels espais privats protegits per la inviolabilitat de l'art. 18.2 CE (ABA, 2003, p. 23).

Des de la STC 22/1984, s'ha afirmat que la protecció constitucional del domicili és “una protección de carácter instrumental, que defiende los ámbitos en que se desarrolla la vida privada de la persona”. La mateixa sentència segueix considerant que “a través de este derecho no sólo es objeto de protección el espacio físico en sí mismo considerado, sino lo que en él hay de emanación de la persona y de la esfera privada de ella” (GARRÓS, 2005, p. 220).

No obstant això, la inviolabilitat del domicili no es redueix a una protecció solament física. La garantia de la inviolabilitat del domicili també protegeix front a l'observació o vigilància del que succeeix a l'interior del domicili mitjançant aparells de vídeo o d'escolta situats a l'exterior (ETXEBERRIA ET AL., 2011, p. 170). Així, el TC des de la seva més inicial jurisprudència “veda toda clase de invasiones, incluidas las que puedan realizarse sin penetración directa por medio de aparatos mecánicos, electrónicos u otros análogos visuales o auditivos” (STC 22/1984, FJ 5º). De la mateixa manera, la sentència del Tribunal Suprem (a partir d'ara TS), de 5 de Novembre de 1996 reconeix expressament que:

“No estarían autorizados, sin el oportuno plázet judicial, aquellos medios de captación de la imagen o del sonido que filmaran escenas en el interior del domicilio prevaleciéndose de los adelantos y posibilidades técnicas de estos aparatos grabadores, aun cuando la captación tuviera lugar desde emplazamientos alejados del recinto domiciliario” (FJ 5º).

Així doncs, la protecció constitucional que es garanteix a l'art. 18.2 CE es concreta en dues regles. La primera defineix la seva "inviolabilitat", la qual constitueix un autèntic dret fonamental de la persona. És una garantia d'aquest dret la immunitat de l'àmbit privat de la persona de qualsevol tipus d'invasió o agressió exterior d'altres persones o de l'autoritat pública, incloses les que puguin realitzar-se sense penetració física, és a dir, per mitjà d'aparells mecànics, electrònics o anàlegs. La segona regla suposa una aplicació concreta de la primera, i estableix que només serà constitucionalment legítima l'entrada en el domicili efectuada amb consentiment del titular o a l'empara d'una resolució judicial (GARRÓS, 2005, p. 220).

El contingut del dret fonamental és negatiu. El què es garanteix és la facultat del titular d'excloure a terceres persones d'aquest àmbit reservat, i prohibir l'entrada o permanència en ell de qualsevol persona o de l'autoritat pública. Els límits constitucionals a la inviolabilitat domiciliària tenen un caràcter rigorosament taxatiu (GARRÓS, 2005, p. 220).

D'altra banda, cal destacar l'íntima relació que existeix entre el dret a la intimitat i a la inviolabilitat del domicili. La protecció de l'espai privat on es desenvolupen les vivències personals i familiar, els comportaments i les relacions personals, és una prolongació o projecció de la tutela que la Constitució depara al dret a la intimitat. Podem afirmar que la inviolabilitat domiciliària no només es configura com un dret, sinó també com una garantia a la intimitat (ABA, 2003, p. 25).

La LO 4/1997 prohibeix la utilització de la videovigilància per obtenir imatges o sons de l'interior dels domicilis, "excepte consentiment del titular o autorització judicial" (art. 6.5). Afegeix que "les imatges i sons obtinguts accidentalment en aquests casos hauran de ser destruïts immediatament".

El TS ha dictat sentència de 20 d'abril de 2016 en la que estableix que la observació d'una vivenda amb prismàtics per part de la Policia, sense autorització judicial, vulnera el dret a la inviolabilitat del domicili. En efecte:

"la tutela constitucional del derecho proclamado en el apartado 2 del art. 18 de la CE protege, tanto frente la irrupción in consentida del intruso en el escenario doméstico, como respecto de la observación clandestina de lo que acontece en su interior, si para ello es preciso valerse de un artificio técnico de grabación o aproximación de las imágenes" (STS 326/2016, FJº 2).

“La protección constitucional de la inviolabilidad del domicilio, cuando los agentes utilizan instrumentos ópticos que convierten la lejanía en proximidad, no puede ser neutralizada con el argumento de que el propio morador no ha colocado obstáculos que impidan la visión exterior” (STS 326/2016, FJº 2).

Afegeix que interpretar que unes persianes no baixades o unes cortines no corregudes pel habitant transmeten una autorització implícita per a l'observació de l' interior de l'immoble, suposa el risc d'afeblir de manera irreparable el contingut material del dret a la inviolabilitat domiciliària. Per tant, la intimitat no desapareix pel simple fet de que el titular o usuari de la vivenda no reforci els elements d'exclusió associats a qualsevol immoble.

Com es pot observar, els supòsits en que s'admet la utilització de la videovigilància són els mateixos que estableix l'art. 18.2 CE en relació a la inviolabilitat del domicili: el consentiment del titular o autorització judicial. Per tant, la protecció que garanteix la LO 4/1997, en relació a la inviolabilitat del domicili, és idèntica a la constitucional (ETXEBERRIA ET AL., 2011, p. 170).

En definitiva, les entrades no consentides pel titular del domicili, o no autoritzades judicialment, constitueixen una violació d'aquest espai privat, però no es requereix la penetració física, essent suficient la captació de les activitats o comportaments que es realitzen en el seu interior per constituir una ingerència en el dret fonamental (ABA, 2003, p. 25). Tal i com remarca el TS, “la protección constitucional frente a la incursión en un domicilio debe abarcar, ahora más que nunca, tanto la entrada física del intruso como la intromisión virtual” (STS 326/2016).

3. La videovigilància en l'àmbit laboral

En l'ordenament jurídic espanyol no existeix una normativa específica que reguli la instal·lació i utilització de sistemes de captació d'imatges o gravació de sons com a mecanismes de control i vigilància per part de l'empresari. Davant tal absència, la referència legal que podem entendre aplicable és l'art. 20.3 ET, en virtut del qual l'empresari podrà, en l'exercici de les seves funcions de control i direcció de l'activitat laboral, adoptar les mesures de vigilància i control que estimi més oportunes per a verificar el compliment per part del treballador de les obligacions i deures laborals (RODRÍGUEZ, 2001, p. 191). Així ho legitima l'ET, establint com a límits la consideració deguda a la dignitat humana del treballador, i en el seu cas, la capacitat real dels treballadors disminuïts (ETXEBERRIA ET AL., 2011, p. 50).

Aquest article permet, doncs, a l'empresari l'establiment de mesures de vigilància per controlar la prestació de serveis del treballador. La lectura d'aquest precepte permet advertir sobre l'existència de dos limitacions clares en l'exercici d'aquesta facultat (GUDE, 2015, p. 6). En primer lloc, els controls han de tenir com a objectiu inspeccionar l'execució de les obligacions laborals, sense excedir de qüestions que excedeixin del desenvolupament de la mateixa. Només abasta els aspectes que guardin relació directa amb la prestació de serveis i el lloc de treball, i qualsevol extralimitació es considerarà il·legítima. El segon límit es refereix a la dignitat humana (GUDE, 2015, p. 6).

Al mateix temps, encara que de forma més indirecta, el propi ET estableix un requisit a l'efecte en l'art. 64.1.4.d), segons el qual el comitè d'empresa ha d'emetre un informe previ a l'execució per part de l'empresari de les decisions adoptades per aquest, sobre la implantació o revisió de sistemes d'organització i control del treball (RODRÍGUEZ, 2001, p. 191). Aquest dret exigeix a l'empresa que informi als representants dels treballadors amb quinze dies d'antelació per a que aquests emetin informe³ en tal termini. L'empresari ha de comunicar les pautes d'instal·lació de les càmeres, com es realitzarà el control, quins són els objectius, la gravació o no de les imatges i l'accés a, conservació i cancel·lació de les mateixes, etc (ETXEBERRIA ET AL., 2011, p. 51).

No obstant, pot matisar-se que els tribunals han admès la instal·lació de sistemes de videovigilància sense comunicació prèvia als treballadors o als seus representants, sense

³ No obstant, aquest informe no és vinculant per a l'empresa (VIDAL, 2014, p. 3).

complir per tant amb el dictat art. 64.1.4.d) ET, quan tal comunicació posi en perill l'objectiu que persegueix, si aquest es verificar el comportament irregular d'un treballador (STC 186/2000). La OIT, en el repertori de recomanacions pràctiques *Protecció de les dades personals dels treballadors* (1997) manté que el secret en matèria de videovigilància només s'ha de permetre quan la seva realització estigui permès per la legislació nacional, i existeixin sospites suficients d'activitat delictiva o altres infraccions greus (ETXEBERRIA ET AL., 2011, p. 59).

3.1 El conflicte entre el poder de direcció de l'empresari i els drets dels treballadors

L'empresari, per virtut del contracte de treball, ostenta un poder de supervisió i control que actua sobre les prestacions laborals que es desenvolupen dins la mateixa. Aquest poder pot adoptar múltiples formes, però degut al desenvolupament de les noves tecnologies, la videovigilància s'ha convertit en l'actualitat en un mecanisme que permet a l'empresari un ple i excel·lent control no només del seu patrimoni, sinó també de l'activitat laboral dels seus treballadors, assegurant la bona marxa de l'organització i detectant actituds fraudulentess o deslleials (ETXEBERRIA ET AL., 2011, p. 50).

El poder de direcció empresarial és una potestat contractual que deriva i forma part del contingut essencial de la llibertat d'empresa, reconeguda constitucionalment en l'art. 38 CE, i que resulta "imprescindible para una buena marcha de la organización productiva" (STC 98/2000 i STC 186/2000) (RODRÍGUEZ, 2001, p. 186). Aquestes facultats empresarials de vigilància i control sobre els treballadors han de desenvolupar-se de forma correcta, lleial i ajustant-se a les causes concretes que les justifiquen (GUDE, 2015, p. 3). Per tant, no estem parlant d'un poder que és absolut, sinó que té com a límit el respecte als drets fonamentals dels treballadors (RODRÍGUEZ, 2001, p. 186).

En aquest sentit, el TC ha assenyalat que el desenvolupament d'aquestes potestats de l'empresari, en cap cas pot comportar la producció de resultats inconstitucionals o lesius dels drets fonamentals dels treballadors (STC 94/1984). Per tant, els drets suposen un límit general a les facultats organitzatives i controladores de l'empresari (STC 90/1997). D'aquesta manera, la STC 88/1985, FJ 2º, insisteix en que "la celebración de un

contrato de trabajo no puede implicar en modo alguno la privación por una de las partes, el trabajador, de los derechos que la Constitución le reconoce”, afegint la STC 99/1994, FJ 4º, que “la relación contractual no puede convertirse en un título legitimador de recortes en el ejercicio de los derechos fundamentales del trabajadores como ciudadano, que no pierde su condición de tal insertarse en el ámbito de una organización” (GUDE, 2015, p. 4).

En aquesta mateixa línia, altres resolucions de l’Alt Tribunal recullen la idea de que les facultats directives reconegudes a l’art. 38 del text constitucional i desenvolupades a l’ET, no imposen a aquells que presten serveis, per compte i sota la dependència dels seus titulars, que hagin de suportar restriccions o limitacions arbitràries i injustificades dels seus drets constitucionals i llibertats públiques (GUDE, 2015, p. 4 i RODRÍGUEZ, 2001, p. 187).

En efecte, una vegada fixada pel TC l’afirmació de que la llibertat d’empresa no faculta a l’empresari per establir limitacions injustificades en els drets fonamentals i llibertats públiques dels treballadors, aquest matisa que, la relació contractual implica una modulació en l’exercici de tals drets, de forma que (RODRÍGUEZ, 2001, p. 188).

“Aunque la celebración de un contrato de trabajo no implica en modo alguno que el trabajador quede privado de los derechos que la Constitución le reconoce como ciudadano, la existencia de una relación contractual entre trabajador y empresario genera un complejo de derechos y obligaciones recíprocas que modula el ejercicio de los derechos fundamentales, de manera que manifestaciones de los mismos que en otro contexto pudieran ser legítimas no tienen porque serlo necesariamente dentro del ámbito de esa relación contractual ⁴” (STC 4/1996, FJ 4º).

Així doncs, la relació laboral comporta l’existència de drets i obligacions tant pel treballador com per a l’empresari, que necessàriament han de conciliar-se, sent un deure bàsic del treballador, com assenyala l’art. 5.a) ET “complir amb les obligacions concretes del seu lloc de treball, de conformitat amb les regles de la bona fe i diligència” (RODRÍGUEZ, 2001, p. 188).

La limitació dels drets fonamentals del treballadors només es produirà “en la medida estrictamente imprescindible para el correcto y ordenado desarrollo de la actividad

⁴ Altres manifestacions de drets fonamentals que es poden veure modulades en el marc d’una relació laboral són la llibertat d’expressió o el dret a la pròpia imatge. En aquest sentit v. SSTC 120/1983 [RTC 1983\120], 88/1985 [RTC 1985\88], 6/1988, 129/1989 [RTC 1989\129], 126/1990, 99/1994 [RTC 1994\99] i 6/1995 [RTC 1995\6].

productiva” (STC 99/1994), la qual cosa exigeix al jutge una ponderació adequada entre el dret fonamental en joc i les obligacions laborals que poden modular-lo (STC 106/1996) (FERNÁNDEZ, 2000, p. 10).

En conclusió, pot reiterar-se que els drets fonamentals es veuen modulats en l'àmbit de les relacions laborals, per la qual cosa la facultat de control i vigilància empresarial pot resultar legítima en detriment de tals drets, sempre i quan la seva utilització tinguin una finalitat exclusivament laboral (RODRÍGUEZ, 2001, p. 193).

De la jurisprudència assentada pel TC pot deduir-se que, davant el conflicte entre els drets fonamentals dels treballadors i els poders de l'empresari, el TC fixa una regla de preferència condicionada en favor dels primers, que s'imposen sobre els segons sempre que actuïn de bona fe i, en tant que del propi objecte del contracte no es derivi necessàriament la restricció del dret fonamental (FERNÁNDEZ, 2000, p. 10).

3.2 Requisites

3.2.1 El principi de proporcionalitat

Davant tal xoc d'interessos, el TC ha consagrat i acceptat el principi de proporcionalitat com a element eix per resoldre tal conflicte. Serà el principi de proporcionalitat en la seva versió de triple judici el que decideixi, en cada cas concret, si és acceptable o no la restricció de drets fonamentals que provoca la videovigilància en el centre de treball.

Segons la jurisprudència constitucional, aquest principi és:

“Una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia a los derechos a la integridad física y a la intimidad” (STC 207/1996, FJ 4º).

El principi de proporcionalitat requereix el compliment de tres requisits o condicions: “si las cámaras son aptas para conseguir el objetivo o fin perseguido” (judici d'idoneïtat); si, a més, són necessàries, en el sentit que no existeixen altres mesures més moderades per a la consecució de tal propòsit amb igual eficàcia (judici de necessitat); i, finalment, “si son ponderadas o equilibradas, derivándose de las mismas más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en

conflicto”(judici de proporcionalitat en sentit estricte) (STC 186/2000, FJ 4º) (GUDE, 2015, p. 16).

a) El judici d'idoneïtat o adequació

La mesura adoptada per l'empresari ha de ser apta per aconseguir l'objectiu o fi perseguit (GUDE, 2015, p. 17). Aquest primer element té forma de regla jurídica, en el sentit de que obliga a rebutjar aquelles vies que no siguin idònies per aconseguir una determinada finalitat, i es basa en consideracions fàctiques (GUDE, 2015, p. 16):

“L'adequació o inadequació no depèn de les seves conseqüències jurídiques o de la major o menor incidència en àmbits constitucionalment protegits, sinó únicament en la seva capacitat per aconseguir la finalitat perseguida” (GONZALEZ, 2003, p. 125).

D'aquesta manera, superar aquest primer subprincipi suposa establir si l'instrument és apte per assolir el fi o objectiu pel qual ha sigut creat, o bé, en termes del TC, si “tal mesura era susceptible d'aconseguir l'objectiu proposat” (GOÑI, 2005, p. 82).

Per tant, la mesura d'utilització de videovigilància decidida per l'empresari ha de ser apta per aconseguir el fi o objectiu perseguit (ETXEBERRIA ET AL., 2011, p. 56). El TC dóna per vàlid aquest requisit quan, existint sospites raonables de la comissió per part del treballador de greus irregularitats en el seu lloc de treball, l'empresari opta per establir un circuit tancat de televisió, ja que resulta idònia per a “verificar si el trabajador cometía efectivamente las irregularidades sospechadas y en tal caso, adoptar las medidas disciplinarias correspondientes” (STC 186/2000).⁵

Per últim, cal afegir que l'únic objectiu de la instal·lació de les càmeres de videovigilància ha de ser únicament verificar les sospites, mai interposar-se en la intimitat dels treballadors (ETXEBERRIA ET AL., 2011, p. 57).

⁵ En aquest sentit, v. també STSJ País Basc 25 de setembre de 2001, STSJ Astúries 22 de març de 2002 i STSJ Castella La Manxa de 23 de desembre de 2005.

b) El judici de necessitat

En aquest cas, l'òrgan judicial haurà de constatar si la restricció al dret fonamental és estrictament indispensable per emparar la facultat que ha legitimat la seva adopció. El TC utilitza, en aquest judici, un cànon que s'identifica amb la imprescindibilitat de la mesura, i suposa que els instruments de vigilància empresarial només seran legítims en aquells casos que resultin indispensables (GOÑI, 2005, p. 83).

El judici de necessitat requereix que la necessitat de la mesura limitadora impliqui l'exigència d'acreditar que la mesura restrictiva proposada és indispensable per la consecució de la finalitat (GUDE, 2015, p. 17).

Si existissin altres mitjans alternatius a la proposta, que complissin la funció amb la mateixa eficàcia, i al mateix temps no restringissin els drets fonamentals dels treballadors, llavors, l'instrument empresarial proposat seria innecessari i desproporcionat. Per consegüent, el judici de necessitat resultarà negatiu quan la decisió empresarial sigui l'alternativa més greu entre totes les possibles (GUDE, 2015, p. 17).

En aquest sentit, la mesura es considerada com a *ultima ratio*. Al respecte, el TC manté que existint raonables sospites de la comissió de irregularitats fraudulentes en el desenvolupament de l'activitat d'un treballador, la gravació es converteix en prova de les mateixes ⁶ (STC 186/2000) (GUDE, 2015, p. 17).

c) El judici de proporcionalitat en sentit estricte

Per últim, l'ús de la videovigilància ha de fer-se de manera ponderada o equilibrada (ETXEBERRIA ET AL., 2011, p. 57). Tal i com ha manifestat el TC, una mesura restrictiva de drets fonamentals és proporcionada “cuando deriven de ella más beneficios y ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto” (STC 66/1995, FJ 5º). En altres termes, és precís que existeixi un cert equilibri entre els

⁶ V. STJSM 84/2015, de 9 de febrer. Aquesta coneix en segona instància de l'acomiadament improcedent d'un treballador després de constatar, mitjançant la instal·lació d'un sistema de videovigilància, que l'actor guardava el material desaparegut en un armari adjunt al seu lloc de treball, per després treure'l fora de les instal·lacions de l'empresa.

En aquest cas, la necessitat és negada pel recurrent al·legant que podria haver-se utilitzat un registre, però no explica perquè un registre en la persona del treballador és menys invasiu que una gravació d'imatges, a part de que aquesta mesura de control és menys idònia ja que, si resulta fallida en un primer registre, resulta clar que el treballador culpable ja queda alertat.

beneficis que s'obtenen per la protecció del dret fonamental, valor o fi que motiva la limitació del dret fonamental i els perjudicis que se'n deriven pel dret que s'ha vist limitat (GUDE, 2015, p. 18).

Aquest criteri requereix dur a terme una ponderació, d'una banda, entre la gravetat o intensitat de la vulneració en el dret fonamental, i de l'altra, el pes de les raons que la justifiquen (GUDE, 2015, p. 18). A diferència del judici d'idoneïtat, ambdós elements no s'analitzen des de la perspectiva de la causalitat, sinó comparant la seva respectiva entitat o pes (GONZALEZ, 2003, p. 133).

En aquest sentit, el TC exigeix que la gravació es limiti a zones comunes i a una duració temporal limitada. Respecte les zones comunes, el judici de proporcionalitat exigeix que el control per videovigilància es restringeixi a l'àmbit físic imprescindible, sense que sigui possible un control genèric de tot l'espai laboral. Tampoc poden controlar-se lloc especialment íntims o protegits pel dret a la intimitat (taquilles, banys, dutxes, ...⁷). En quant al temps, quedaria prohibida la instal·lació de càmeres de forma permanent en el centre de treball (ETXEBERRIA ET AL., 2011, p. 57).

En definitiva, si es compleixen els tres judicis esmentats que conformen el principi de proporcionalitat, la videovigilància en el centre de treball estarà justificada i no serà

⁷ La resolució R/00259/2010, de 8 de març, de l'AEPD s'ocupa de la instal·lació d'una videocàmera en els banys d'un centre educatiu: "Aunque pueda resultar justificable el uso de técnicas de videovigilancia por motivos de seguridad, en ningún caso resulta admisible la instalación de cámaras en baños por la naturaleza de los derechos fundamentales que pueden verse afectados, entre los que se encuentra el de la protección de datos, debiendo tenerse en cuenta tal circunstancia a fin de respetar tales derechos y no captar imágenes de personas identificadas o identificables en dichos lugares, tal y como se ha comprobado ocurrió en los cuatro baños en que se usaron dispositivos de videovigilancia. Por lo tanto, se trataba de un tratamiento particularmente invasivo e intrusivo para la intimidad de las personas titulares de los datos tratados y para el derecho de disposición de los propios datos de los afectados, ya que la medida utilizada, aunque fuera susceptible de cumplir el objetivo de prevención frente a actos vandálicos en los bienes del centro, no era ponderada ni equilibrada por derivarse de ella perjuicios sobre los derechos de terceros en conflicto" (FJ 8º).

També, la resolució R/02091/2013, de l'AEPD entén que: "Se han instalado 13 cámaras que abarcan distintas zonas de las instalaciones: (aparcamiento, zona de acceso a los vestuarios, zonas de paso a las dependencias policiales, sala de denuncias, sala de descanso en la que se encuentra el armario). Con las cámaras pueden captarse imágenes susceptibles de afectar a los derechos de intimidad, a la propia imagen y a la protección de los datos, puesto que en el ángulo de visión de la cámara situada en el área de descanso aparece una mesa de la zona de descanso, lo que debe considerarse un tratamiento excesivo y no proporcional de las imágenes, que supone una vulneración del art. 4 de la LOPD" (FJ 7º).

arbitrària, esdevenint un instrument legítim de control de l'activitat laboral (ETXEBERRIA ET AL., 2011, p. 57). Els tribunals laborals acudeixen, per valorar la licitud de les càmeres de vídeo en el lloc de treball, al principi de proporcionalitat sotmetent la seva utilització a un judici de ponderació. En conseqüència, la valoració dels jutges en aquest àmbit és decisiva, ja que es deixa en les seves mans la consideració de licitud o il·licitud de la mesura en cada cas concret (GUDE, 2015, p. 18).

3.2.2 Interès legítim

Es fa referència a legitimació per al·ludir a la justificació de l'ús de les tècniques de videovigilància tant des de la perspectiva de l'existència d'un fi legítim com del criteri de proporcionalitat (DESDENTADO & MUÑOZ, 2012, p. 63). Tot tractament de dades personals ha d'estar legitimat per alguna de les causes de l'art. 6 LOPD. Doncs bé, la captació i gravació de les imatges dels treballadors en el centre de treball amb un fi de control laboral apareix emparat per l'art. 6 LOPD, al existir una habilitació legal de caràcter imperatiu per a "les parts d'un contracte ... d'una relació negocial, laboral o administrativa i quan sigui necessari per al seu manteniment o compliment" (AEPD, 2014, p. 2).

L'exigència d'una finalitat legítima en el tractament de dades, prevista en l'art. 4.1 LOPD, ve donada, en l'àmbit de la videovigilància laboral, per les facultats de control empresarial que reconeix l'art. 20.3 ET, sempre i quan aquestes s'exerceixin dins del seu àmbit legal i no lesionin els drets fonamentals del treballador (ALVAREZ, 2015, p. 6). En aquest sentit, l'art. 20.3 ET en relació amb l'art. 6 LOPD legitimaria, en principi, a l'empresari per tractar les imatges dels treballadors en l'àmbit laboral amb caràcter general (AEPD, 2014, p. 3).

Així ho ha vingut reiterant la jurisprudència, com és el cas de la sentència del TS de 2 de juliol de 2007:

"Desde luego, la finalidad perseguida mediante su utilización es plenamente legítima: el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos. Y, en tanto esa obligación es inherente a la relación que une a estos con la Administración Autonómica, no es necesario obtener previamente su consentimiento ya que el artículo 6.2 LOPD lo excluye en estos" (FJ 7º).

La Instrucció 1/2009, de l'APDCAT, exigeix dins el seu àmbit territorial de competència, a més, en el seu art. 10, l'elaboració d'una memòria amb caràcter previ a la posada en marxa del sistema de videovigilància, el contingut de la qual ha de referir-se a la justificació de la finalitat i de la proporcionalitat del sistema, entre d'altres (ALVAREZ, 2015, p. 7).

Ara bé, aquesta legitimació no és absoluta i exigeix que l'empresari informi de tal tractament als treballadors (complint així amb el deure d'informació previst tant en l'art. 13 del Reglament (UE) 2016/679 com en l'art. 5 LOPD), el qual serà tractat en el pròxim apartat. I no només als propis treballadors, sinó també als seus representants (AEPD, 2014, p. 3).

3.2.3 Deure d'informació i principi de consentiment

La Instrucció 1/2006 de l'AEPD estableix en el seu article 3 que els responsables que comptin amb sistemes de videovigilància hauran de complir amb el deure d'informació previst a l'art. 5 LOPD. Amb tal fi, hauran de col·locar, a les zones videovigilades, almenys, un distintiu informatiu ubicat en un lloc suficientment visible, així com tenir a disposició dels interessats impresos en els que es detalli la informació prevista en l'art. 5.1 LOPD (GUDE, 2014, p. 57).

El contingut i disseny del distintiu informatiu s'ajustarà segons el que preveu l'Annex d'aquesta Instrucció. L'AEPD no disposa de cap criteri sobre quines han de ser les dimensions mínimes del cartell informatiu de la videovigilància, únicament que s'ha d'ajustar a l'espai en que es vagi a col·locar. Respecte la ubicació, no es necessari que es situï sota de la càmera, sinó que serà suficient, d'acord amb l'art. 3.a) de la Instrucció 1/2006, situar-lo en un lloc suficientment visible tant en espais oberts com tancats (AEPD, 2007, p. 1) (GUDE, 2014, p. 57). S'ha de tenir en compte que el lloc vigilat disposa de varis accessos, s'ha de col·locar en tots aquells a l'objecte de que la informació sigui visible, amb independència de per a quin lloc s'accedeixi. L'AEPD assenyala, també, que el cartell s'ha de trobar dins el camp de visió natural de l'afectat, a l'altura dels ulls (ALVÁREZ, 2014, p. 8).

Segons disposa l'art. 6.1 LOPD, el consentiment de l'afectat per al tractament de dades serà inequívoc, excepte quan la llei disposi una altra cosa. Aquest principi queda anul·lat pel punt 2 del mateix precepte, que exceptua de tal consentiment aquells supòsits en que el tractament es refereixi a les parts d'un contracte d'una relació negocial, laboral o administrativa. Es presumeix que la formalització del vincle jurídic permet també la recollida i tractament de dades i, per tant, és possible la captació de les imatges sense cap altre tipus de pronunciament exprés, sempre i quan les imatges obtingudes tinguin una finalitat exclusivament de seguretat o control laboral (GUDE, 2014, p. 57). En conseqüència:

“El principi d'autodeterminació informativa no impedeix el tractament de dades del treballador per l'empresari, el coneixement del qual és precís per a l'establiment i manteniment de la relació laboral” (GUDE, 2014, p. 58).

Si bé el consentiment del treballador no es necessari per procedir a la gravació de la seva imatge, sí és imprescindible que l'empresari informi sobre l'ús que va a fer-se de les seves dades, sent el contracte el mitjà idoni per a tal finalitat (GUDE, 2014, p. 61). La jurisprudència ordinària s'ha pronunciat sobre la transcendència d'aquest deure, “porque es el que permite llevar a cabo el ejercicio de otros derechos, y así lo valora el texto positivo al pormenorizar su contenido y establecer la exigencia de que el mismo sea expreso, preciso e inequívoco” (SAN 15 de juny de 2001). De la mateixa manera, és necessari citar les paraules del TC, referint-se a la importància del deure d'informació dels treballadors quan es procedeix a la recollida de les seves dades personals:

“De suerte que, sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia...” (STC 292/2000, FJ 6º).

No obstant, la més recent jurisprudència dictada pel TC aclareix la seva doctrina en relació a l'ús de càmeres de videovigilància en l'empresa. En sentència de data de 3 de Març de 2016, el TC estableix que la instal·lació del distintiu informatiu de “Zona videovigilada”, regulat per la Instrucció 1/2006, per una empresa a l'entrada del seu establiment, compleix amb l'obligació d'informació prèvia al treballador de la instal·lació de tals sistemes. Segons assenyala el Tribunal, aquesta sentència té especial transcendència ja que permet aclarir l'abast de la informació a facilitar als treballadors

sobre la finalitat de l'ús de la videovigilància en l'empresa: si és suficient la informació general o, al contrari, ha d'existir una informació específica (tal com s'havia pronunciat la STC 29/2013).

En compliment d'aquesta obligació, l'empresa va col·locar el corresponent distintiu a l'entrada de la botiga on prestava els serveis la treballadora, per la qual cosa aquesta podia conèixer l'existència de les càmeres i la finalitat per la que havien sigut instal·lades. S'ha complert en aquest cas amb l'obligació d'informació prèvia, ja que el distintiu és suficient a aquests efectes per al compliment dels requisits d'informació a, d'acord amb la Instrucció 1/2006. El treballador coneixia que s'havia instal·lat un sistema de videovigilància, sense que s'hagi d'especificar, més enllà de la mera vigilància, la finalitat exacta que se li ha assignat a tal control. El que és important és determinar si les dades obtingudes s'han utilitzat per a la finalitat de control de la relació laboral o per una finalitat aliena al contracte de treball. En el cas de la segona opció, l'empresari estaria obligat a sol·licitar el consentiment dels treballadors afectats (STC 39/2016, FJ 4º).

En conseqüència, el TC resol que:

“Teniendo la trabajadora información previa de la instalación de las cámaras de videovigilancia mediante el correspondiente distintivo informativo, y habiendo sido tratadas las imágenes captadas para el control de la relación laboral, no puede entenderse vulnerado el artículo 18.4 CE “(STC 39/2016, FJ 5º).

En efecte, aquesta nova sentència suposa un canvi de criteri pel que respecta al deure d'informació del dret a l'autotutela informativa. La doctrina constitucional fixada en l'anterior STC 29/2013 assenyalava que:

“No contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la AEPD; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo” (FJ 8º).

No obstant, ara s'afirma amb rotunditat que:

“La colocación en el escaparate del establecimiento, en un lugar visible, del distintivo informativo genérico (exigido por la Instrucción 1/2006 de la AEPD), hace presumir que la trabajadora podía conocer de la existencia de las cámaras y la finalidad para la que estas habían sido instaladas” (STC 39/2016, FJ 4º).

El nou criteri adoptat en aquesta sentència no es compartit per tots els magistrats del TC, doncs s’afegeixen dos vots particulars que discrepen del contingut de la resolució, els quals consideren que s’havia de declarar la nul·litat de l’acomiadament perquè la instal·lació de les videocàmeres es va realitzar sense informar la treballadora de la seva finalitat concreta i, per tant, va vulnerar el seu dret a la pròpia imatge (art. 18.4 CE).

De la mateixa manera, Rojo es suma al vot particular emès pel magistrat Fernando Valdés perquè creu que situa amb plena exactitud els termes d’un debat que va molt més enllà del cas concret jutjat:

“Pero esta mutación jurisprudencial no solo me parece objetable por la forma; lo es, sobre todo, por el fondo. Anticipando la conclusión final que he de desarrollar en breve, la doctrina ahora defendida se sitúa en esa senda, para mí preocupante, de retroceso en la protección de los derechos fundamentales de las personas que prestan un trabajo asalariado y que vengo denunciando en los últimos años a través de una sucesión de votos particulares. Una senda que revela una orientación que tiende a vaciar de contenido sustantivo un modelo constitucional de relaciones laborales acorde con el Estado social y democrático de Derecho (art. 1.1 CE)”.

Tal i com conclou Tovar Rocamora, la present sentència ha flexibilitzat – potser en excés – els límits que, en matèria de drets fonamentals, els empresaris tenien en l’exercici de les seves potestats disciplinàries i de control.

3.3 Drets ARCO

Com a regla general, la LOPD reconeix a tots els ciutadans una sèrie de drets, coneguts sota l’acrònim de ARCO, i que no són altres que els drets d’accés, rectificació, cancel·lació i oposició, els quals tenen plena efectivitat en l’àmbit de la videovigilància. Aquests formen part, tal i com ha manifestat la jurisprudència constitucional, del contingut essencial del dret fonamental a la protecció de dades i són, en definitiva, drets subjectius de caràcter personal que hauran de ser exercitats directament davant el responsable del fitxer, tant si es tracta d’una persona pública com privada (GUDE, 2014, p. 78).

3.3.1 Dret d'accés

El dret d'accés, exponent del que s'anomena *habeas data*, és un dret personalíssim⁸ i una garantia d'institut⁹ per l'exercici d'altres drets fonamentals. D'acord amb l'art. 15 LOPD, l'interessat, en aquest cas la persona objecte de videovigilància, tindrà dret a sol·licitar i obtenir gratuïtament informació sobre les imatges sotmeses a tractament, el seu origen i les comunicacions realitzades amb elles. El RLOPD també inclou dins el contingut essencial d'aquest dret la potestat de l'interessat a obtenir informació sobre la finalitat del tractament del material (GUDE, 2014, p. 78).

No obstant, excepcionalment el responsable del fitxer podrà oposar-se al dret d'accés del titular a les imatges. No es tracta, per tant, d'un dret absolut, sinó que podrà ser denegat quan concorrin determinades circumstàncies¹⁰ (GUDE, 2014, p. 78).

La informació requerida es podrà obtenir mitjançant visualització en pantalla, escrit, còpia o fotocòpia enviada per correu, certificada o no, telecòpia, correu electrònic o qualsevol altre mitjà adient a la configuració o implantació material del fitxer. L'AEPD, en l'informe jurídic 0193/2007, es va pronunciar respecte que la LOPD “no exigeix cap sistema en concret, quedant per tant, a l'elecció del consultant” (GUDE, 2014, p. 79).

El dret d'accés del treballador per comprovar si s'ha respectat el fi pel qual van ser captades haurà d'exercitar-se en intervals no inferiors a dotze mesos, excepte que l'interessat acrediti un interès legítim, cas en el qual es podrà efectuar amb anterioritat. Així ho estableix l'art. 15.3 LOPD (GUDE, 2014, p. 79).

⁸ Per la qual cosa només podrà sol·licitar-lo la persona interessada.

⁹ La “garantia institucional” és una categoria originada els anys vint per la doctrina alemana, amb la que es persegueix la protecció davant el legislador de determinades institucions que es recullen *in nuce* a la CE. La garantia institucional vindria a ser aquella protecció constitucional que preserva a una institució no només de la seva destrucció, sinó de la seva desnaturalització, al prohibir vulnerar la seva imatge mestra. Aquest és el seu significat comú, que en un principi es circumscriu a institucions públiques (institucions en sentit estricte – es parla així de garanties “institucionals” – o garanties “d'institució” –), però després es projecta sobre institucions privades (instituts – es parla així de garanties “d'institut” –) i inclús sobre determinades manifestacions socials (es parla així de garanties d'institucions socials) (CIDONCHA, 2009, p. 150).

En l'article 18.4 CE s'exigeix al legislador que limiti l'ús de la informàtica per garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets. Es troba en aquest mandat un institut de garantia d'altres drets, principalment l'honor i la intimitat, però aquest institut és al mateix temps (en sí mateix) un dret o llibertat fonamental, l'anomenada llibertat informàtica, entesa com el dret a controlar l'ús de les dades incloses en un programa informàtic (*habeas data*). Es tracta, doncs, d'un ens amb doble naturalesa: una garantia d'institut i un dret fonamental (CIDONCHA, 2009, p. 155).

¹⁰ Per exemple, en aquells casos que sigui necessari protegir drets i llibertats de tercers, quan sigui precís assegurar la repressió de conductes o infraccions molt greus en l'empresa o aquelles situacions en les que els esforços per recuperar les imatges resultin desproporcionats en matèria d'investigació, cost i recursos si es comparen amb la brevetat del període de retenció de les mateixes.

Segons l'art. 25.1.a) RLOPD, per a l'exercici del dret d'accés i per a la resta de drets ARCO, la sol·licitud haurà de contenir: nom i cognoms de l'interessat, així com fotocòpia del DNI, passaport o document identificatiu vàlid. El termini per respondre la petició d'accés és, segons l'art. 29.1 RLOPD, d'un mes a comptar des de la recepció. Transcorregut aquest temps sense resolució expressa, s'entendrà desestimada (GUDE, 2014, p. 79).

3.3.2 Drets de rectificació i cancel·lació

La LOPD contempla els drets de rectificació i cancel·lació que pot exercir l'interessat en el mateix precepte, l'art. 16. L'exercici del dret de rectificació dóna lloc a la substitució de dades errònies per les correctes, per adequar el tractament a la situació real de la persona interessada. La cancel·lació, d'altra banda, busca l'eliminació de les dades (GUDE, 2014, p. 80). No obstant, en aquest cas no resulta possible l'exercici del dret de rectificació, ja que per la naturalesa de les dades –imatges gravades de la realitat que reflecteixen un fet objectiu- es tractaria de l'exercici d'un dret de contingut impossible (ALVÁREZ, 2014, p.13). L'art. 16.2 LOPD preveu dos supòsits de rectificació o cancel·lació de dades.

Primer, quan el tractament no s'ajusti al principi de seguretat establert a la LOPD. En aquest cas, en la majoria dels supòsits procedeix la cancel·lació degut a que, probablement, la captació i tractament de les imatges s'ha realitzat de manera il·legal. L'art. 4.5 LOPD exigeix la cancel·lació quan les imatges deixin de ser necessàries o pertinents per al propòsit pel qual van ser recollides. Al respecte, la Instrucció 1/2006 fixa en l'art. 6 el termini d'un mes per a la seva cancel·lació¹¹. No es pot associar el terme “cancel·lar” amb el terme “destruir”, ja que l'exercici del dret de cancel·lació únicament requereix conservar les imatges degudament bloquejades per tal d'evitar el seu tractament (art. 16.3 LOPD), però això no implica la seva desaparició física. Finalitzat el termini legal sí es procedirà a la supressió dels fitxers. El conseqüència, el termini d'un mes que fixa la Instrucció 1/2006 és el període màxim de cancel·lació de les imatges en els termes vistos (bloqueig del material per evitar el seu ús), no per a la seva eliminació i destrucció que estarà subjecta al transcurs dels terminis de prescripció

¹¹ L'AEPD ha seguit el mateix criteri que l'establert en l'art. 8 LO 4/1997.

de les responsabilitats. Les còpies de seguretat es sotmetran als mateixos terminis (GUDE, 2014, p. 80-81).

El segon supòsit es produeix quan les dades o, en aquest cas les imatges, siguin inexactes o incompletes. La cancel·lació haurà de fer-se efectiva en un període màxim de deu dies des de la recepció de sol·licitud de l'interessat, sempre i quan no existeixi una obligació legal de conservació davant les autoritats judicials o policials per captació d'un il·lícit penal. Després de la sol·licitud de cancel·lació es procedirà al bloqueig de les gravacions (GUDE, 2014, p. 81).

El responsable del fitxer podrà denegar els drets de rectificació i cancel·lació en determinats supòsits: quan el sol·licitant sigui una persona diferent al titular de les imatges i no quedi acreditat que actua en representació d'aquest (art. 23 RLOPD); quan així ho estableixi una llei o norma de dret comunitari (art. 33.2 RLOPD); si les imatges han de ser conservades durant un termini determinat en virtut d'una norma o en virtut de les relacions contractuals entre l'entitat responsable i l'interessat que van justificar el tractament de dades (art. 33.1 RLOPD)¹²; i, en aquelles situacions en que es pogués causar un perjudici a interessos legítims de l'afectat o tercers (Norma Tercera, punt 5 RLOPD) (GUDE, 2014, p. 82).

3.3.3 Dret d'oposició

El dret d'oposició és el dret de l'afectat a que no es dugui a terme el tractament de les dades o al cessament del mateix en els supòsits previstos (DESDENTADO & MUÑOZ, 2012, p. 65). De la mateixa manera que el dret de rectificació, no es possible l'exercici del dret d'oposició, ja que si aquest s'interpreta com la impossibilitat de gravar imatges d'un subjecte concret en el marc d'instal·lacions de videovigilància vinculades a fins de seguretat privada no resultaria possible la seva satisfacció en la mesura que prevaldria la protecció de la seguretat (ALVAREZ, 2015, p. 13).

¹² L'AEPD, en la resolució R/02696/2011, avala que la relació contractual existent impedeix la cancel·lació de les dades personals, i desestima la reclamació efectuada per la part actora. Així, "en el supuesto aquí analizado, queda acreditado que el reclamante ejercitó su derecho de cancelación ante la entidad demandada, y que, dentro del plazo establecido conforme a las normas antes señaladas, la entidad motiva las causas por las que no procede la cancelación al existir una relación contractual entre las partes y que obliga a la entidad a mantener los datos personales del reclamante" (FJ. 6º).

En base a tot el que s'ha exposat anteriorment, es poden individualitzar els requisits exigibles per a la instal·lació de càmeres de vigilància i la seva utilització per fins laborals i disciplinaris en el centre de treball:

- 1) Acreditació de la necessitat d'instal·lar càmeres, és a dir, que es tracti d'una mesura imprescindible. La jurisprudència del TC exigeix, a més, que la mesura sigui proporcional. Per tant, la instal·lació de les videocàmeres ha de ser equilibrada amb les necessitats de l'empresa (VIDAL, 2014, p. 3).
- 2) Realitzar gravacions exclusivament en l'àmbit físic estrictament imprescindible, per assegurar el respecte dels drets fonamentals del treballador, i molt especialment del dret a la intimitat personal que protegeix l'art. 18.1 CE, tenint en compte sempre el principi de proporcionalitat (STC 186/2000) (VIDAL, 2014, p. 3).
- 3) Deure de comunicació i informació als treballadors i als seus representants legals sobre la mesura implantada, tal i com exigeix l'art. 64 ET.

Per últim, els sistemes de videovigilància només poden utilitzar-se per satisfer la finalitat que va justificar la seva adopció. D'aquesta manera, se'n deriva la impossibilitat d'exercir el poder disciplinari per sancionar incompliments que no estiguessin relacionats amb la finalitat anunciada en el moment de la instal·lació d'aquest mecanisme de control (VIDAL, 2014, p. 3).

Conclusions

Una vegada finalitzat tot el que s'ha exposat anteriorment, sembla ser que les noves tecnologies de la informació i la comunicació han tingut un fort impacte en la cultura, costums i pràctiques actuals. La videovigilància s'ha convertit en un fenomen molt comú en la nostra societat, i està present en tot tipus d'entorns, tant de l'àmbit públic com de l'àmbit privat. Bancs, hospitals, carreteres, empreses, domicilis, transports públics i infinitat d'altres llocs es troben vigilats constantment sota la mirada d'un ull electrònic. Aquesta elevada presència de videocàmeres pot estar justificada per diferents motius. En la majoria de casos, es deu a fins de seguretat per a la protecció de béns i persones i/o a fins de control. No obstant, gràcies a l'auge d'aquest tipus de sistemes, la videovigilància també ha trobat altres aplicacions en la promoció turística, investigacions, estudis conductuals, etc.

El progrés i el desenvolupament tecnològic han elevat exponencialment l'eficiència de la videovigilància, convertint-la en un instrument de control potencialment restrictiu, ja que actualment no es limita només a la captació i gravació de imatges i sons, sinó que també ofereix moltes altres possibilitats, com ara el zoom i ampliació de imatges, reconeixement facial, lectura de matrícules, entre d'altres.

La introducció de les noves tecnologies en l'àmbit empresarial també ha transformat les relacions laborals, contribuint a la reducció de costos, augmentant la rapidesa en la prestació de serveis i, sobretot, introduint nous mecanismes d'inspecció, com les videocàmeres. Això crea un debat sobre la inserció d'instruments tecnològics en la prestació de serveis i els conflictes que origina el seu ús amb l'exercici dels drets fonamentals dels treballadors tan importants com la intimitat, la pròpia imatge i la protecció de dades. En la meua opinió, cadascú defensa la postura que és més beneficiosa pels seus interessos.

L'absència d'una regulació expressa sobre videovigilància empresarial en el nostre ordenament jurídic contrasta amb el seu ús cada vegada més freqüent en aquest àmbit, ja que s'ha convertit en una eina altament eficaç per garantir la seguretat, prevenir els delictes i controlar la prestació del treball. Altres països del nostre entorn, en canvi, estableixen en la seva legislació una prohibició absoluta quan s'implanta amb la finalitat de control laboral (és el cas d'Itàlia o Portugal), o bé requereixen l'observació de certs

requisits com la transparència, proporcionalitat i consulta prèvia als representants dels treballadors (és el cas de França i Alemanya). No obstant, considero necessari remarcar que en els darrers dos últims mesos hi ha hagut una activitat legislativa força important en aquesta matèria. D'una banda, el TC va dictar sentència el 3 de març mitjançant la qual s'introdueix un canvi de criteri pel que fa al deure d'informació de l'empresari i, de l'altra, el 27 d'abril es va publicar el nou Reglament (UE) 2016/679 de protecció de dades (pel que es deroga la Directiva 95/46/CE).

L'art. 20.3 ET habilita a l'empresari a adoptar les mesures que estimi més oportunes de vigilància, i legitima, per tant, la instal·lació de sistemes de videovigilància en el centre de treball. També, la LOPD (fruit de la transposició de la Directiva Europea 95/46/CE) i el seu reglament de desenvolupament, juntament amb la Instrucció 1/2006 de l'AEPD constitueixen les normes bàsiques que regulen aquesta matèria en el dret espanyol.

Davant la gairebé inexistència normativa de la matèria en l'àmbit laboral, són els tribunals els que estan responenent per protegir els drets fonamentals del treballador davant el poder de direcció que ostenta l'empresari. Per tant, aquests s'han encarregat de configurar i delimitar la seva instal·lació i utilització en el marc del centre de treball. Inicialment, afirmaven que les càmeres no suposaven cap amenaça ja que el dret a la intimitat no es podia exercir en el centre de treball. A partir de la STC 90/2000 i 186/2000 es va produir un canvi de criteri, introduint la tècnica de la ponderació per a valorar la intromissió o no de les videocàmeres en els drets fonamentals dels treballadors.

Per jutjar la legitimitat de l'instrument de videovigilància, la jurisprudència sotmet la mesura al criteri de proporcionalitat, en la seva triple vessant: judici d'adequació, judici de necessitat i judici de proporcionalitat en sentit estricte. Així doncs, s'estudien les circumstàncies concretes en cada cas, però aquesta situació dona una elevada capacitat de decisió als tribunals, i pot arribar a provocar una sensació d'ambigüitat i inseguretat a les parts. En la meua opinió, seria desitjable establir un mecanisme objectiu de compliment que entri a valorar la legalitat de la mesura de cara a consolidar la seguretat jurídica.

L'empresari, a més, ha de complir amb una sèrie de deures. Tal i com he comentat, la recent STC 39/2016 ha suposat un canvi transcendental en relació a l'obligació d'informació prèvia, en la mesura que suposa una redefinició de l'abast del contingut essencial del dret fonamental a la protecció de dades. A partir d'ara, la simple fixació

del distintiu informatiu en un lloc visible dóna per complerta aquesta obligació d'informació prèvia, mentre que la seva sentència anterior STC 29/2013 exigia una informació prèvia expressa, precisa, clara i inequívoca. La nova sentència suposa un canvi radical respecte la seva antecessora, i a mode de crítica considero que seria necessari una valoració clara, coherent i definitiva pel que respecta a drets fonamentals, i així evitar la sensació d'inseguretat jurídica que aquests canvis d'interpretació poden provocar.

Per tant, en resposta a la hipòtesi formulada a l'inici de l'estudi, he de concloure, que si l'empresari s'ajusta al criteri de proporcionalitat (en la seva triple vessant) i compleix amb els deures i obligacions que té en matèria de protecció de dades, la instal·lació del sistema de videovigilància serà plenament legítima, prevalent el poder de direcció de l'empresari per sobre els drets dels treballadors.

És evident que els canvis en aquest àmbit es produeixen molt ràpidament, i el ritme del legislador no acompanya a l'avanç tecnològic. Per això, considero que la negociació col·lectiva ha de desenvolupar un paper fonamental en relació a l'ús de les tecnologies de la informació i comunicació en l'àmbit laboral, ajudant a cercar solucions respectuoses amb els drets fonamentals dels treballadors i definint drets i obligacions de les parts del contracte de treball en aquest nou món tecnològic. Crec que la intervenció de diferents actors socials (sindicats, empresaris, juristes, etc.) seria una forma d'omplir la mancança de legislació existent, i han de ser capaços de fixar pautes de desenvolupament i de solució de conflictes en aquests casos.

Estudis han demostrat que aquest control ininterromput i constant té efectes negatius sobre els treballadors, augmentant els nivells de desconfiança, desmotivació, pressió i estrès. Per tant, crec que també és important, en aquesta nova realitat tecnològica, la necessitat d'actuar conforme al principi de la bona fe, i informar al treballador d'aquells instruments tecnològics dels quals és objecte de control.

Bibliografia

ABA CATOIRA, A. (2003). La videovigilància i la garantía dels drets individuals: el seu marc jurídic. *Anuario da Faculta de de Dereito da Universidade da Coruña*, núm. 7, pp. 13-36.

ÁLVAREZ HERNANDO, J. (2014). *Videovigilancia*. En *Practicum Protección de Datos 2015* (pp. x). Pamplona: Aranzadi.

-- (2015). *Relaciones laborales y protecciones de datos*. En *Practicum Protección de Datos 2015* (pp. x). Pamplona: Aranzadi.

ARZOZ SANTISTEBAN, X. (2002). Videovigilancia y derechos fundamentales: Análisis de la constitucionalidad de la Ley Orgánica 4/1997. *Revista Española de Derecho Constitucional*, núm. 64, pp. 133-176.

CHAPARRO, P. i TALENS, E. (2013). Las intromisiones en el derecho a la propia imagen en el ámbito laboral. *Revista de derecho*, núm. 15, pp. 234-251.

CIDONCHA MARTÍN, A. (2009). Garantía institucional, dimensión institucional y derecho fundamental: balance jurisprudencial. *Teoría y realidad constitucional*. Núm. 23, pp. 149-188.

DESDENTADO BONETE, A. i MUÑOZ RUIZ, A. B. (2012). *Control informático, videovigilancia y protección de datos en el trabajo*. Valladolid: Lex Nova.

GARRÓS FONT, I. (2005). La videovigilància i el control de les garanties constitucionals (Tesis doctoral, Universitat Autònoma de Barcelona, 2005). *La videovigilància i el control de les garanties constitucionals*, 467.

ETXEBERRIA GURIDI, J. F., ORDEÑANA GEZURAGA, I., ARZOZ SANTISTEBAN, X., CALONGE CRESPO, I., ESPARZA LEIBAR, I., GONZÁLEZ LÓPEZ, J. J., PECHARROMÁN FERRER, B., PÉREZ GIL, J., SUBIJANA ZUNZUNEGUI, I. J. (2010). *Videovigilancia: Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de los datos personales*. València: Tirant Lo Blanch.

FERNÁNDEZ ESTEBAN, M. L. (2000). Estudio de la jurisprudencia constitucional y ordinaria sobre el secreto a las comunicaciones entre particulares, en especial en el ámbito de la empresa. *Revista Doctrinal Aranzadi Civil*, núm. 1, pp. 1883-1918.

GONZALEZ BEILFUSS, M. (2003). *El principio de proporcionalidad en la Jurisprudencia del Tribunal Constitucional*. Pamplona: Aranzadi.

GOÑI SEIN, J. L. (2005). Los criterios básicos de enjuiciamiento constitucional de la actividad de control empresarial: debilidad y fisuras del principio de proporcionalidad. *Revista Derecho Social*, núm. 32, pp. 79-102.

-- (2007). *La videovigilancia empresarial y la protección de datos personales*. Madrid: Thomson Civitas.

-- (2009). Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos. *Justicia laboral: revista de derecho del trabajo y de la seguridad social*. Núm. 39, pp. 11-58.

GUDE FERNÁNDEZ, A. (2014). La videovigilancia laboral y el derecho a la protección de datos de carácter personal. *Revista de Derecho Político UNED*, núm. 91, pp. 43-90.

-- (2015). La videovigilancia en el ámbito laboral y el derecho a la intimidad. *Revista General de Derecho Constitucional*, núm. 20, pp. 109-134.

IBARRA SANCHEZ, E. (2011). *Videovigilancia: punto de colisión entre derechos fundamentales, seguridad y protección de datos personales*. En *Jurismática. El derecho y las nuevas tecnologías* (pp. 231-269). Monterrey: Universidad Autónoma de Nueva León.

IZUEL CARCAVILLA, E. (2004). Videovigilancia en seguridad privada: problemática y exámen del vacío legal existente en la normativa española. *Sentencias de TSJ, AP y otros Tribunales*, núm. 3, pp. 15-32.

RODRÍGUEZ COARASA, C. (2001). Algunas proyecciones del derecho constitucional a la intimidad en el ámbito laboral. *Revista de Derecho Político*, núm. 51, pp. 183-222.

RODRÍGUEZ COPÉ, M. L. (2001). El derecho a la intimidad del trabajador como límite al poder de dirección empresarial. *Temas Laborales. Revista Andaluza de Trabajo y Bienestar Social*, núm. 62, pp. 213-228.

RUBIO SÁNCHEZ, F. (2003). Derecho a la intimidad de los trabajadores: Vigilancia con cámaras de seguridad u otro tipo de dispositivos. *Revista doctrinal Aranzadi Social*, núm. 17, pp. 419-423.

SEGOVIANO ASTABURUAGA, M. L. (2004). El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores. *Revista jurídica de Castilla y León*, núm. 2, pp. 145-187.

VIDAL, P. (2014). La utilización de las cámaras de videovigilancia para fines disciplinarios y de control del trabajo. *Actualidad Jurídica Aranzadi*, núm. 888, pp. 1-3.

Webgrafia

Agència Espanyola de Protecció de Dades. (2007). *Informe jurídic 0084/2007 Cartell informatiu*. Recuperat 16 abril 2016, des de https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/videovigilancia/common/pdfs/2007-0084_Cartel-informativo.pdf

Agència Espanyola de Protecció de Dades. (2014). *Informe jurídic 0475/2014*. Recuperat 3 abril 2016, des de https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdf_destacados/2014-0475_Sistema-de-videovigilancia-en-guarder-ii-a-para-control-laboral.pdf

Agència Espanyola de Protecció de Dades. (2014). *Guía de Videovigilancia*. Recuperat 27 febrer 2016, des de https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf

Alvarez Hernando, J. (2010). *Ley Omnibus y videovigilancia*. Recuperat 29 març 2016, des de <http://alvarezabogado.blogspot.com.es/2010/03/ley-omnibus-y-videovigilancia.html>

Aritio, A. (2014). *Videovigilancia y la nueva Ley de Seguridad Privada*. Recuperat 29 març 2016, des de <http://www.audea.com/videovigilancia-y-la-nueva-ley-de-seguridad-privada/>

Constitució Espanyola, de 1978 (BOE, [en línia], núm. 311, 29-12-1978). < <https://www.boe.es/buscar/pdf/1978/BOE-A-1978-31229-consolidado.pdf> > [Consulta: 2 març 2016].

Diario La Ley. *Vulneración de la inviolabilidad del domicilio por la observación policial con prismáticos de una vivienda sin autorización judicial*. Recuperat 13 maig 2016, des de <http://diariolaley.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAkNDQxNLY7Wy1KLizPw8WyMDQzMDUwMTkEBmWqVLfnJIZUGqbVpiTnEqAChOwR81AAAAWKE>

Directiva 95/46/CE, del Parlament Europeu i del Consell, de 24 d'Octubre de 1995, relativa a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades (DOUE L, núm. 281, 23-11-1995, pp. 31-50). < <https://www.boe.es/doue/1995/281/L00031-00050.pdf> > [Consulta: 24 febrer 2016]

D-Link. (2010). *Regulación normativa de la videovigilancia*. Recuperat 1 març 2016, des de <http://www.videovigilanciadlink.es/d-link-normativas-videovigilancia-01-03-2011-pdf>

Instituto Nacional de Tecnologías de la Comunicación INTECO. (2011). *Guía sobre videovigilancia y protección de datos personales*. Recuperat 4 març 2016, des de [file:///C:/Users/user/Downloads/guia_videovigilancia_2011%20\(1\).pdf](file:///C:/Users/user/Downloads/guia_videovigilancia_2011%20(1).pdf)

Instrucció 1/2006, de 8 de Novembre, de l'Agència Espanyola de Protecció de Dades, sobre el tractament de dades personals amb fins de vigilància a través de sistemes de càmeres o videocàmeres (BOE [en línia], núm. 296, 12-12-2006, pp. 43458-43460). < <https://www.boe.es/boe/dias/2006/12/12/pdfs/A43458-43460.pdf> > [Consulta: 23 febrer 2016]

Instrucció 1/2009, de 10 de Febrer, sobre el tractament de dades de caràcter personal mitjançant càmeres amb fins de videovigilància (DOGC [en línia], núm. 5.322, 19-2-2009, pp. 13258-13272). < <http://www.apd.cat/media/664.pdf> > [Consulta: 25 febrer 2016]

Llei 5/2014, de 4 d'Abril, de Seguretat Privada (BOE [en línia], núm. 83, 5-4-2014, pp. 28975-29024). <<https://www.boe.es/boe/dias/2014/04/05/pdfs/BOE-A-2014-3649.pdf> > [Consulta: 28 febrer 2016]

Llei Orgànica 1/1982, de 5 de Maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge (BOE [en línia], núm. 115, 14-5-1982, pp. 12546-12548). < <https://www.boe.es/boe/dias/1982/05/14/pdfs/A12546-12548.pdf> > [Consulta: 5 març 2016]

Llei Orgànica 4/1997, de 4 d'Agost, per la que es regula la utilització de videocàmeres per les forces i cossos de seguretat en llocs públics (BOE [en línia], núm. 186, 5-8-

1997, pp. 23824-23828). < <https://www.boe.es/boe/dias/1997/08/05/pdfs/A23824-23828.pdf> > [Consulta: 10 març 2016]

Llei Orgànica 15/1999, de 13 de Desembre, de Protecció de Dades de Caràcter Personal (BOE [en línea], núm. 298, 14-12-1999, pp. 43088-43099). < <https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf> > [Consulta: 23 febrer 2016]

OIT. (1997). *Protección de los datos personales de los trabajadores*. Recuperat 24 març 2016, des de http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf

Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'Abril de 2016, relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades i pel que es deroga la Directiva 95/46/CE (DOUE L, núm. 119, 4-5-2016, pp. 1-88). < <http://www.boe.es/doue/2016/119/L00001-00088.pdf> > [Consulta: 5 maig 2016]

Reial Decret 596/1999, de 16 d'Abril, pel que s'aprova el Reglament de desenvolupament i execució de la Llei Orgànica 4/1997, de 4 d'Agost, per la que es regula la utilització de videocàmeres per les Forces i Cossos de Seguretat en llocs públics (BOE [en línea], núm. 93, 19-4-1999, pp. 14555-14561). < <https://www.boe.es/boe/dias/1999/04/19/pdfs/A14555-14561.pdf> > [Consulta: 10 març 2016]

Reial Decret 1720/2007, de 21 de Desembre, pel que s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de Desembre, de protecció de dades de caràcter personal (BOE [en línea], núm. 17, 19-1-2008, pp. 4103-4136). < <https://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf> > [Consulta: 23 febrer 2016].

Reial Decret Legislatiu 2/2015, de 23 d'Octubre, pel que s'aprova el text refós de la Llei de l'Estatut dels Treballadors (BOE [en línea], núm. 255, 24-10-2015, pp. 100224-100308). < <https://www.boe.es/boe/dias/2015/10/24/pdfs/BOE-A-2015-11430.pdf> > [Consulta: 25 febrer 2016]

Reial Decret Legislatiu 5/2000, de 4 d'Agost, pel que s'aprova el text refós de la Llei d'Infraccions i Sancions de l'Ordre Social (BOE, [en línea], núm. 189, 8-8-2000, pp.

28285-28300). < <https://www.boe.es/boe/dias/2000/08/08/pdfs/A28285-28300.pdf> >
[Consulta: 19 abril 2016]

Rojo, E. (2016). *Después de las Jornadas Catalanas de Derecho Social. ¿Constitucionalización del poder de dirección empresarial en la relación de trabajo? Nota crítica a la sentencia del Tribunal Constitucional de 3 de marzo de 2016 (sobre instalación de cámaras de videovigilancia) (I)*. Recuperat 20 abril 2016, des de <http://www.eduardorojotorrecilla.es/2016/03/despues-de-las-jornadas-catalanas-de.html>

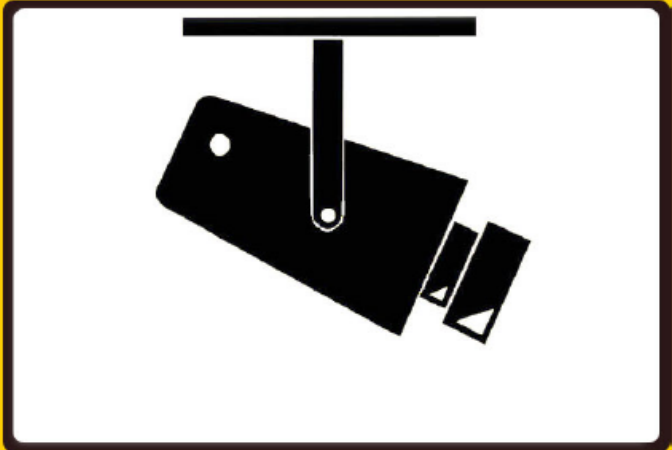
Sempere, F. J. (2014). *Nueva Ley de Seguridad Privada y su incidencia en la protección de datos*. Recuperat 14 març 2016, des de <http://www.privacidadlogica.es/2014/04/07/nueva-ley-de-seguridad-privada-y-su-incidencia-en-proteccion-de-datos/>

Tovar Rocamora, J. J. (2016). *Comentario a la STC, de 3 de marzo de 2016, en materia de sistemas de videovigilancia en el ámbito laboral*. Recuperat 20 abril 2016, des de <https://archivolaboral.org/2016/03/31/comentario-a-la-stc-de-3-de-marzo-de-2016-en-materia-de-sistemas-de-videovigilancia-en-el-ambito-laboral/>

Annexos

Annex I - Model de cartell informatiu segons la Instrucció 1/2006, de 8 de novembre, de l'AEPD

ZONA VIDEOVIGILADA



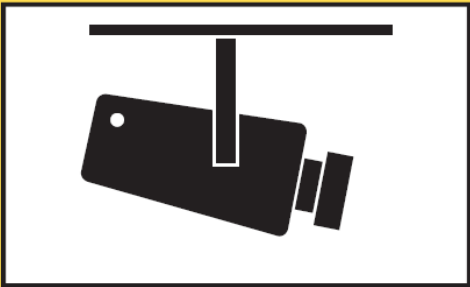
LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS

PUEDE EJERCITAR SUS DERECHOS ANTE:

**Annex II - Models de cartells informatius segons la Instrucció 1/2009,
de 10 de febrer, de l'APDCAT**

apdcat

ZONA VIDEOVIGILADA

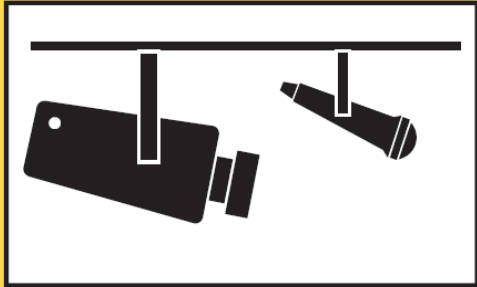


PROTECCIÓ DE DADES
POT EXERCIR ELS SEUS DRETS DAVANT:

PER A MÉS INFORMACIÓ:

apdcat

ZONA VIDEOVIGILADA



PROTECCIÓ DE DADES
POT EXERCIR ELS SEUS DRETS DAVANT:

PER A MÉS INFORMACIÓ:

Annex III - Escrit per a comunicar als treballadors la instal·lació de càmeres de videovigilància en el centre de treball

Por medio de la presente les informamos de que la empresa _____, S.A., va a proceder a la instalación de cámaras de videovigilancia en el centro de trabajo con los fines de vigilancia y control, tal y como se señala a continuación.

Respecto al tratamiento de datos de imágenes en el lugar de trabajo, el artículo 20.3 del Estatuto de los Trabajadores dispone que «El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso».

El tratamiento de las imágenes por _____, en su calidad de responsable del tratamiento, le obliga –de acuerdo con lo establecido en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de videovigilancia a través de sistemas de cámaras o videocámaras– a cumplir con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la Ley 15/1999, de 13 de diciembre, y en la precitada Instrucción 1/2006, de 8 de noviembre. Con este objeto se incluirán carteles informativos, utilizando el modelo proporcionado por la Agencia Española de Protección de Datos, en distintos lugares de la empresa.

Les informamos de que, atendiendo a lo establecido en la LOPD, usted, como interesado, tiene derecho de acceso y cancelación a los ficheros de videovigilancia de la empresa. De todo ello han sido informados los representantes de los trabajadores.

Para que así conste a todos los efectos.

D./Dña. _____, Director/a de Recursos Humanos.

Annex IV - Escrit per a comunicar als representants dels treballadors sobre la instal·lació de càmeres de videovigilància en el centre de treball

Por medio de la presente les informamos de que la empresa _____, S.A., va a proceder a la instalación de cámaras de videovigilancia en el centro de trabajo, de acuerdo con lo establecido en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de videovigilancia a través de sistemas de cámaras o videocámaras.

Respecto al tratamiento de datos de imágenes en el lugar de trabajo, el artículo 20.3 del Estatuto de los Trabajadores dispone que «El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso».

Tal y como han manifestado la Agencia Española de Protección de Datos y numerosas Sentencias del Tribunal Supremo, la aplicación del artículo 20.3 del Estatuto de los Trabajadores legitima a la empresa, aun sin contar con el consentimiento de los trabajadores, en caso de que los afectados hayan sido debidamente informados de la existencia de esta medida, debiendo además ser claro que, conforme a lo exigido por el artículo 4.2 de la Ley Orgánica 15/1999, de 13 de diciembre (en adelante, LOPD), los datos no podrán ser utilizados para fines distintos.

Por tanto, el tratamiento de las imágenes por _____, S.A., en su calidad de responsable del tratamiento, le obliga a cumplir con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la LOPD. Con este objeto se incluirán carteles informativos en distintos lugares de la empresa, además de facilitarse dicha información a cada uno de los trabajadores, mediante una circular interna.

Por otro lado, la normativa exige su comunicación a los representantes de los trabajadores, en tanto que el artículo 64.1 ET dispone que «El comité de empresa tendrá derecho a ser informado y consultado por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores...», y en el punto 5 que «El comité de

empresa tendrá derecho a emitir informe, con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por éste, sobre las siguientes cuestiones: f) La implantación y revisión de sistemas de organización y control del trabajo, estudios de tiempos, establecimiento de sistemas de primas e incentivos y valoración de puestos de trabajo».

Para que así conste a todos los efectos.

D./Dña. _____, Director/a de Recursos Humanos.