UNIVERSITAT DE BARCELONA
Facultat de Dret

PROTECCIÓ DE DADES EN L'ÀMBIT LABORAL:

La política d'empresa sobre l'ús del correu electrònic

Treball final de grau

Dirigit per Dra. Esther Mitjans Perelló

Laura Farrés Font

Maig 2014

A la Dra. Esther Mitjans Perelló,
per la seva col·laboració, interès i ajuda professional.

Als professors que he tingut al llarg de la carrera,
per formar-me i enriquir-me professionalment.

A en Joan Pedrosa Gutiérrez,
per les seves recomanacions i crítiques com a assessor en protecció de dades.

Als meus pares,
per donar-me suport en tot moment i per fer-me ser jo.

A en Toni,
per ser qui és i per fer-me seguir endavant.

ÍNDEX D'ABREVIATURES

AEPD	Agència Espanyola de Protecció de Dades
APDCAT	Autoritat Catalana de Protecció de Dades
CE	Constitució Espanyola de 1978
CEDH	Conveni Europeu de Drets Humans
CP	Codi Penal
EAC	Estatut d'Autonomia de Catalunya
ET	Real Decret Legislatiu 1/1995, de 24 de març, pel que s'aprova el text refós de la Llei de l'Estatut dels Treballadors.
GT 29	Grup de Treball de l'article 29
LOPD	Llei Orgànica 15/1999 de Protecció de Dades de Caràcter Personal
SAN	Sentència de l'Audiència Nacional
SSAN	Sala Social de l'Audiència Nacional
STC	Sentència del Tribunal Constitucional
STHDE	Sentència del Tribunal Europeu de Drets Humans
STSJ	Sentència del Tribunal Superior de Justícia
STS	Sentència del Tribunal Suprem
TC	Tribunal Constitucional
TEDH	Tribunal Europeu de Drets Humans
TS	Tribunal Suprem
TSJC	Tribunal Superior de Justícia de Catalunya
TSJM	Tribunal Superior de Justícia de Madrid

ÍNDEX

INTRODUCCIÓ

La protecció de dades no ha estat mai considerada com un dels drets més rellevants per la societat, no obstant, any rere any ha anat prenen més importància en la nostre vida i sobretot en l'àmbit laboral. En aquest sentit es poden destacar tres impactes a nivell mundial que han repercutit en la protecció de dades, i aquests són:

1. Les tecnologies de la informació i la comunicació.
2. La delinqüència i el terrorisme, ja que per seguretat s'ha establert un control policial i de vigilància.
3. La investigació biomèdica ja que ha permès la manipulació de dades genètiques. (Oró, 2008)

Per aquest motiu, he considerat oportú realitzar una recerca sobre l'impacte que ha tingut i té actualment la protecció de dades en l'àmbit de les empreses i veure l'ús que en fan els empresaris. Si bé és cert que els empresaris, segons l'article 20 del Real Decret Legislatiu 1/1995, de 24 de març, pel que s'aprova el text refós de la Llei de l'Estatut dels Treballadors, en endavant ET o Estatut dels Treballadors, tenen la competència de dirigir i controlar l'activitat laboral, en moltes ocasions aquests extralimiten la seva facultat.

D'altra banda, vull destacar que podem definir el dret a la protecció de dades com el dret a la privadesa o el dret a la protecció de la vida privada. Per tant, el dret a la protecció de dades protegeix a les persones i no a les dades en sí. La Constitució Espanyola, en endavant CE, de 1978 en el seu article 18.4, preveu aquest dret quan *" limita l'ús de la informàtica per garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets ".*

Com a antecedents a la protecció de dades, cal destacar el Conveni 108 del Consell d'Europa signat a Estrasburg el 1981. Va ser el primer conveni en

tractar detalladament la protecció de dades ja que regula uns principis referents al registre i la utilització d'informacions de caràcter personal. Els ciutadans, doncs, poden controlar i decidir sobre la difusió de la informació sobre la seva persona, atès que es protegeix l'individu de la recollida, transmissió o utilització de les seves pròpies dades. Ara bé, aquest només va ser un dels primers instruments que regulava la protecció de dades ja que posteriorment altres instruments, com ara la Carta dels Drets Fonamentals de la Unió Europea del 2000 en el seu article 8, fan referència a la protecció de dades. Així, el dret a la protecció de dades garanteix a l'individu a accedir a les dades sobre la seva persona i a la seva rectificació, que les dades es tractaran de forma lleial i sota el consentiment de l'individu afectat i que les normes referents a la protecció de dades seran tractades per organismes independents.

Com a motivació en la elaboració del treball, he tingut la oportunitat de visitar una empresa formada per diversos experts en l'àmbit de la protecció de dades, que m'ha ajudat a enriquir el treball i a veure des d'un altre punt de vista els criteris que estableixen tant els Tribunals com les diferents autoritats de protecció de dades.

Per últim, vull destacar la metodologia de treball que seguiré. Ja que amb el present treball em proposo com a objecte d'estudi analitzar el paper que té la protecció de dades en les empreses del moment i veure com establir una bona política d'empresa en relació l'ús del correu electrònic, em basaré en la normativa europea i espanyola (com ara la Llei Orgànica 15/1999 de Protecció de Dades de Caràcter Personal) així com en sentències al respecte, tenint en compte que entre la relació jurídica del treball i la protecció de dades sempre trobarem un *element subjectiu* (les parts), un *element objectiu* (les dades) i un *element formal* (el consentiment i la confidencialitat). Per això, contrastaré la jurisprudència relativa a la protecció de dades, i més concretament aquella jurisprudència que tracti temes referents al correu electrònic en les empreses, amb els informes i criteris al respecte del Grup de l'article 29, en àmbit europeu, i de les diferents autoritats de protecció de dades en el nostre país.

1. LA PROTECCIÓ DE DADES COM A DRET FONAMENTAL

La Constitució Espanyola va ser pionera, a través de les peticions dels seus contribuents, en el reconeixement de la protecció de dades com a dret fonamental de tot ciutadà. Va configurar aquest dret en preveure la greu afectació en la intimitat de les persones que el tractament informàtic de dades comportava. No obstant, qui ha definit clarament aquest concepte és el Tribunal Constitucional, en endavant TC, a través de diferents sentències, com per exemple la 254/1993 de 20 juliol que ha estat la primera en configurar el dret.

Pel que fan les característiques derivades de que la protecció de dades sigui considerada un dret fonamental és que és un dret irrenunciable del ciutadà, que ha de desenvolupar-se a través d'una llei orgànica, que té preferència sobre l'exercici d'altres drets considerats no fonamentals i que està protegit i per tant, pot exercir-se davant els Tribunals a través d'un procediment basat en la preferència i la sumarietat (PRODAT[1]).

Encara que la protecció de dades estigui prevista a l'article 18.4 de la CE, la doctrina i essencialment el Tribunal Constitucional, en endavant TC, posen en manifest que existeix un dret inherent i autònom al de la protecció de dades anomenat dret a la llibertat informàtica.

Aquest dret a la llibertat informàtica estaria estrictament lligat a l'article 10.1 de la CE quan nombre el dret a la dignitat, a l'article 18.1 quan estableix el dret a l'honor i a la intimitat personal i familiar, i a l'article 20.1 sobre la llibertat d'expressió i informació.

[1] ***PRODAT:*** *Organització especialitzada en auditoria i consultoria en l'àmbit de la protecció de dades.*

Figura 2: *Imatge que representa la legislació aplicable al dret a la protecció de dades (Font: Generalitat de Catalunya)*

Com veiem, són quatre les normes que regulen aquest dret: L'article 18 de la CE de 1978 en el seu apartat quart, l'Estatut d'Autonomia de Catalunya, en endavant EAC, de 2006 en l'article 31, la Llei Orgànica de Protecció de Dades, en endavant LOPD, i el seu Reglament de desenvolupament 1720/2007. Ara bé, com que el contingut del dret consisteix en controlar en tot moment les dades personals, el dret implica saber qui té informació sobre nosaltres, quina és aquesta informació, d'on prové, per a quina finalitat es tenen les dades i a qui es faciliten.

En definitiva, el límit del dret fonamental de la protecció de dades es troba en l'exercici dels altres drets fonamentals i béns jurídics constitucionalment protegits (Álvarez Civantos, 2008[2]). Així doncs, el dret fonamental a la protecció de dades no té el mateix contingut que el dret a la intimitat, ja que protegeix les dades personals davant el tractament informàtic d'aquestes. No es tracta, doncs, de protegir la intimitat de les persones, sinó de tenir sota control les dades de la nostre persona; en definitiva, les dades no pertanyen a qui les gestiona, sinó al seu titular.

[2] ***Álvarez Civantos, Óscar José:*** *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades. Editorial Comares. Granada (2008).*

En aquest sentit, cal destacar que la doctrina reconèix el dret fonamental a la protecció de dades. Per exemple, Murillo de la Cueva (2006)[3] argumenta que el dret a la intimitat no és suficient per protegir les dades personals, ja que la protecció de dades no empara únicament informació personal reservada, i també argumenta que la rellevància que té el dret a l'honor en aquest àmbit és escassa.

Per últim, vull destacar que per tal de garantir aquest dret a la protecció de dades existeixen diferents organismes encarregats de vetllar pel seu compliment. Aquestes són:

- <u>En l'àmbit nacional:</u>
  - L'Agència Espanyola de Protecció de Dades
  - L'Autoritat Catalana de Protecció de Dades
  - L'Autoritat Basca de Protecció de Dades
- <u>En l'àmbit europeu:</u>
  - L'Autoritat Comuna de Control de Europol
  - L'Autoritat Comuna de Control de Shengen
  - La Comissió Europea
  - El Consell d'Europa
  - El Consell de la Unió Europea
  - El Grup de Treball de l'article 29
  - El Parlament Europeu
  - El Supervisor Europeu de Protecció de Dades
  - El Tribunal de Justícia de la Unió Europea
  - El Consell Europeu

Tot i la rellevància de cadascun d'aquest òrgans, a continuació vull esmentar amb una mica més de detall l'estructura i les funcions de l'Autoritat Espanyola de Protecció de Dades i l'Autoritat Catalana de Protecció de Dades a nivell nacional, i del Grup de Treball de l'article 29 a nivell europeu.

[3] ***Murillo de la Cueva, Pablo Lucas:*** Artícle recollit de la web de l'Autoritat Catalana de Protecció de Dades " Diez preguntas sobre la autodeterminación informativa y la protección de datos de carácter personal "*. Any 2006.*

Pel que fa el **Grup de Treball de l'article 29**, en endavant GT 29, va ser creat per la Directiva Europea 95/46/CE, del Parlament Europeu i el Consell Europeu en data 24 d'octubre de 1995, sobre la protecció dels drets i llibertats de les persones físiques respecte el tractament de dades personals i la lliure circulació dels mateixos. Aquest grup té caràcter d'òrgan consultiu i independent i està integrat per un representant de l'autoritat de control de cada estat membre, pel supervisor europeu de protecció de dades i per un representant de la comissió europea, essent aquesta última qui realitza les funcions de secretària. El GT 29 es reuneix en plenaris amb una periodicitat bimensuals i s'organitza en diferents subgrups de treball per tal d'analitzar aquelles qüestions relatives a la protecció de dades personals. A més, en aquestes reunions hi acudeixen com a observadors els estats candidats a ser membres de la Unió Europea i els països membres de l'EEE. Pel que fa les observacions que fa el GT 29, aquestes es manifesten a través de decisions, dictàmens, documents de treball, informes o recomanacions.

La LOPD, concretament en el seu títol VI, preveu la creació de **l'Agència Espanyola de Protecció de Dades**. Segons la llei, aquesta Agència té la consideració d'ens de dret públic, amb personalitat jurídica pròpia i plena capacitat pública i privada, que actua amb plena independència de les administracions públiques en l'exercici de les seves funcions. Entre les seves funcions generals es troba la de vetllar pel compliment de la legislació sobre protecció de dades i controlar-ne l'aplicació, especialment pel que fa als drets d'informació, accés, rectificació, oposició i cancel·lació de dades. Per últim, i com a caràcter introductori, cal dir que l'AEPD està integrada per:

- ✓ El director: N'és el representant i és nomenat per un període de quatre anys per el Consell Consultiu.
- ✓ El Consell Consultiu: És l'òrgan col·legiat d'assessorament al director.
- ✓ El Registre General de Protecció de Dades: Òrgan integrat a l'Agència encarregat de vetllar per la publicitat dels tractaments de dades.

- ✓ L'inspecció de dades: Les autoritats de control són les que inspeccionen els fitxers i comproven la legalitat dels tractaments de dades.
- ✓ Òrgans corresponents a les comunitats autònomes: Tenen la consideració d'autoritats de control les quals han de garantir la plena independència i objectivitat en l'exercici de la seva tasca.

Figura 1: *Logotip de l'Agència Espanyola de Protecció de Dades*

Foren el Llei 5/2002, de 19 d'abril, de l'Agència Catalana de protecció de Dades i la llei 32/2010, de 1 d'octubre, de **l'Autoritat Catalana de Protecció de Dades** les que preveuen la creació de tal organisme. Segons la llei vigent, és un organisme independent que té per objecte garantir, en l'àmbit de les competències de la Generalitat, els drets a la protecció de dades personals i l'accés a la informació que hi està vinculada. Així, és una institució de dret públic amb personalitat jurídica pròpia i plena capacitat d'obrar per el compliment dels seus fins, amb plena autonomia orgànica i funcional. Entre les seves funcions generals, es troba la de vetllar pel compliment de la legislació vigent sobre protecció de dades de caràcter personal. Cal destacar també, que l'Autoritat Catalana de Protecció de Dades està integrada per dos òrgans de govern:

1. El director: És el representant de la institució i és nombrat per un període de cinc anys, renovables una sola vegada, pel Ple del Parlament per majoria de tres cinquenes parts, a proposta del Consell Assessor de Protecció de Dades. Li correspon dictar resolucions i instruccions, a més d'aprovar les recomanacions i dictàmens que es requereixin.

2. El Consell Assessor de Protecció de Dades: És l'òrgan d'assessorament i participació de l'Autoritat. Està compost per un president, un secretari, tres persones designades pel Parlament, tres persones en representació de la Generalitat, dues persones en representació de l'administració local de Catalunya, una persona experta en drets fonamentals, una persona experta en informàtica, una persona designada per l'Institut d'Estudis Catalans, una persona en representació de les organitzacions de consumidors i usuaris i el director de l'Institut d'Estadística de Catalunya.

Figura 2: *Logotip de l'Autoritat Catalana de Protecció de Dades*

2. LA PROTECCIÓ DE DADES EN LES RELACIONS LABORALS

És una realitat innegable la modernització, any rere any, de les actuals empreses i la introducció de les tècniques de treball i comunicació com a eines de treball pels seus empleats ja que no només en milloren la productivitat, sinó també les condicions de treball. Per això, podem afirmar que avui en dia la tecnologia de la informació i de les comunicacions està afectant cada vegada més a la societat i a les relacions entre els seus habitants (Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics).

Segons Marzo Portera (2009)[4] és aquesta tecnologia la que ha permès als empresaris establir un control electrònic d'entrada i sortida del treballador al centre de treball, de la seva presència al mateix, de les hores treballades, de l'accés a les dades personals o a aplicacions, de la navegació per Internet o fins i tot dels missatges de correu electrònic o de telefonia mòbil rebuts o enviats. No obstant, aquest control empresarial no resulta un control exclusiu pels treballadors, però si que n'acaben sent els més afectats. Per exemple, el control sobre l'ús del correu electrònic pretén vigilar el seu correcte o fraudulent ús i la seguretat o incidències que pugui ocórrer en el mateix.

2.1. PRINCIPIS GENERALS

2.1.1. LA POTESTAT EMPRESARIAL

El poder que es reconeix a l'empresari es pot definir en una sola facultat o en vàries. És a dir, per una banda ens trobem davant el poder de direcció i control de l'activitat laboral previst a l'article 20 de l'Estatut dels Treballadors, i d'altra banda ens trobem en que l'empresari se li reconeixen diferents facultats tals com el poder disciplinari, el poder de vigilància, el poder premial...

[4] ***Marzo Portera, Ana:*** *Vigilancia y control de las comunicaciones electrónicas en el lugar del trabajo. Editorial Ediciones experiència, SL. Barcelona (2009).*

Aquests poders però, s'han anat limitant per la seva naturalesa, continguts i finalitats, a més de l'evolució que ha près i està prenent la normativa laboral.

Aquesta facultat reconeguda, doncs, és imprescindible perquè l'organització productiva de l'empresa funcioni. Per aquesta raó, l'empresari podrà utilitzar la facultat per adoptar les mesures que consideri necessàries per la vigilància i control i així verificar el compliment de les obligacions i deures laborals del treballador. No obstant haurà de respectar sempre la dignitat i intimitat del treballador, tal i com així ho indica l'article 20.3 de l'ET. Ara bé, quan parlem de la potestat empresarial de vigilància i control de l'activitat laboral, indirectament ens referim també a la vigilància dels recursos de treball proporcionats al treballador.

D'altra banda cal destacar que el poder de direcció empresarial té com a límits els drets fonamentals dels treballadors. En aquest sentit, i segons la jurisprudència del TC en la STC 96/2012 de 7 de maig (RTC 2012,96; FJ10), la STC 14/2003, de 28 de gener (RTC 2003,14; FJ9) i la STC 89/2006, de 27 de març (RTC 2006,89; FJ3), els empresaris han d'avaluar la constitucionalitat de qualsevol mesura adoptada. Per tant qualsevol mesura haurà de complir les següents condicions:

- Ha de ser susceptible d'aconseguir l'objectiu que l'empresari s'ha fixat. ***(Judici de idoneïtat)***
- Ha de ser necessària, en el sentit que acrediti que no existeix cap altre mesura a adoptar que sigui igual d'eficient. ***(Judici de necessitat)***
- Ha d'aportar més beneficis que perjudicis. ***(Judici de proporcionalitat en sentit estricte)***

Així doncs, l'objectiu d'aquest control és vetllar per la pròpia activitat laboral i veure la forma d'utilitzar els instruments i recursos de treball. Ara bé, existeixen una sèrie de motius legítims i il·legítims que posen en manifest aquesta facultat, essent els següents:

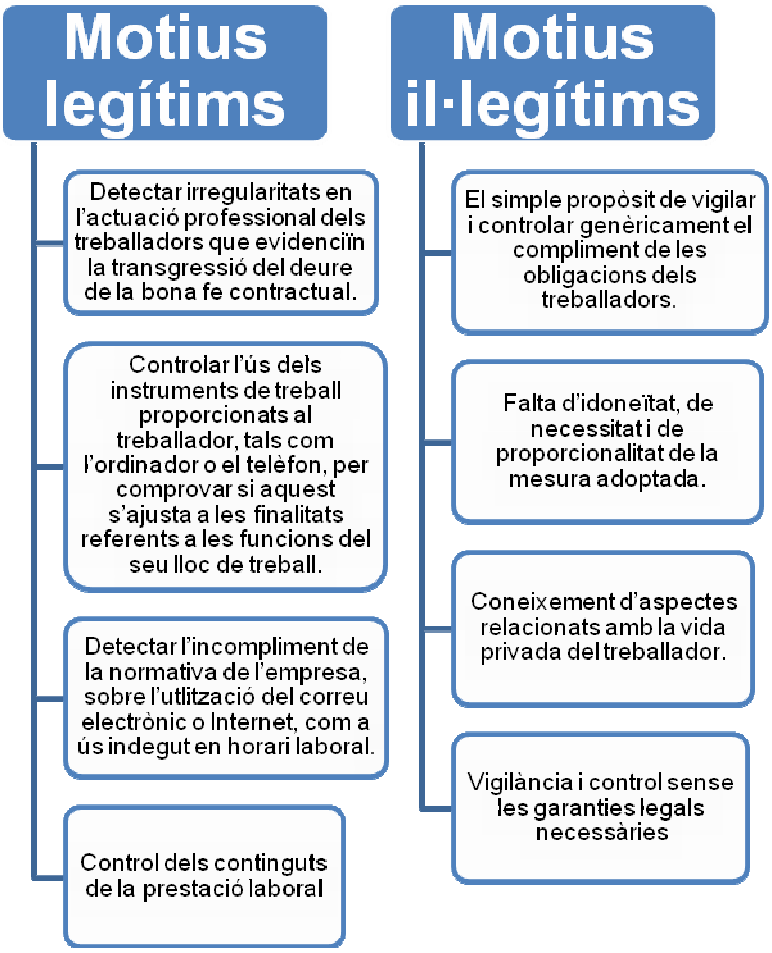

Figura 3: *Gràfic explicatiu dels motius pels quals l'empresari pot executar, o no, la potestat de vigilància i control sobre els seus treballadors. (Marzo Portera, 2009)*

Una altra facultat que es reconeix a l'empresari, segons ho estableix l'article 18 de l'Estatut dels Treballadors referent a la inviolabilitat del treballador, és que podrà registrar al treballador, en els seus armaris i efectes particulars. Ara bé, la mateixa llei també posa límits a aquesta facultat ja que especifica que únicament podrà exercitar-la quan sigui estrictament necessari per la protecció del patrimoni empresarial i dels altres treballadors, durant la jornada laboral i dins el centre de treball. A més a més aquest registre haurà de realitzar-se davant un representant legal dels treballadors o en defecte d'aquest davant un altre treballador de l'empresa, per tal de respectar la dignitat i intimitat del treballador.

Per acabar, cal destacar que els treballadors estan obligats a sotmetre's en aquest poder empresarial ja que deuen a l'empresari diligència i

col·laboració en el treball, tal i com així ho indiquen les disposicions legals següents: l'article 20.2 de l'ET, el Conveni Col·lectiu, les ordres i instruccions de l'empresari i els usos i costums.

2.1.2. EL DEURE DE LA BONA FE DEL TREBALLADOR

Tal i com preveu l'article 5 de l'Estatut dels Treballadors, els treballadors tenen el deure de complir amb les obligacions concretes del seu lloc de treball, de conformitat a les regles de la bona fe i diligència. De no ser així, es produiria un incompliment contractual, per part del treballador, a través de la transgressió de la bona fe contractual i es podria extingir la relació laboral existent entre tal treballador i el seu empresari.

En aquest sentit, cal destacar la jurisprudència del Tribunal Suprem, en sentència de 22 de maig de 1986, quan sustenta que la bona fe és un concepte reconegut en les relacions laborals:

" En el mundo de las relaciones laborales rige el principio básico y fundamental de la buena fe, que en su sentido objetivo constituye un modelo de tipicidad de conducta exigible, o mejor aún, principio general de derecho que impone un comportamiento arreglado a valoracions éticas, que condiciona y limita por ello el ejercicio de los derechos subjetivos, con lo que el prinicpio se convierte en un criterio de valoración de conducas con el que deben cumplirse las obligaciones, y que se traduce en directives equivalentes a lealtad, honorabilidad, probidad y confiança; y es cierto también que en el Derecho Laboral hay mandatos legales que imponent un cumplimiento contractual de acuerdo con la buena fe ".

3. EL CORREU ELECTRÒNIC EN L'EMPRESA COM A INSTRUMENT PROTEGIT

Una característica que diferencia el correu electrònic d'altres mitjans de comunicació és que el contingut d'aquest, a no ser que s'encripti o es protegeixi, pot ser llegit fàcilment pel proveïdor del servei i per aquells que interceptin el missatge, a més del receptor del propi missatge. Per tant, sempre resulta millor utilitzar programes informàtics per tal de garantir la privadesa del seu contingut.

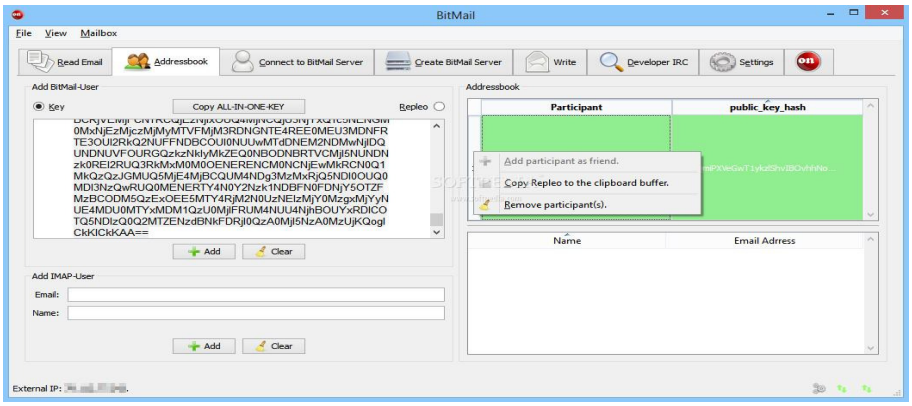

Figura 4: *Imatge del programa informàtic BitMail que mostra com encriptar els missatges d'un correu electrònic.*

En aquest sentit, en l'àmbit laboral la intercepció del missatge pot venir de l'empresari titular de l'ordinador. Ara bé, una de les qüestions a tenir en compte és que quan es fa referència a la vigilància i control que l'empresari pot establir sobre els seus treballadors, en cap moment aquesta vigilància pot establir-se en la intercepció dels continguts de les comunicacions electròniques ja que en aquest cas, es podria vulnerar el dret al secret de les comunicacions del treballador (article 18.3 CE). Així, l'empresari podria realitzar aquesta intercepció mitjançant el registre que preveu l'article 18 de l'Estatut dels Treballadors, sempre que l'ordinador es considerés un efecte personal del treballador, o requerint el missatge al proveïdor del servei del correu electrònic.

Així doncs, el correu electrònic com a instrument que pot afectar al dret al secret de les comunicacions, ha de compatibilitzar-se amb el dret de l'empresari a controlar-ne el seu ús. Alguns autors consideren que ha de ser el

dret fonamental, és a dir, el dret al secret de les comunicacions establert a l'article 18.3 de la CE, el que prevalgui ja que el correu electrònic té una configuració estricta i no permet més modulacions que les previstes expressament en el text constitucional (Marín Alonso 2005)[5]. El treballador té dret, doncs, a que se li respecti la seva vida privada en el treball, no obstant, aquest dret no pot lesionar el dret que té l'empresari a controlar el funcionament de la seva empresa.

3.1. EL PLANTEJAMENT DELS ORGANISMES REFERENTS A LA PROTECCIÓ DE DADES

A continuació es detalla quin és el punt de vista dels diferents organismes, encarregats de garantir la protecció de dades de caràcter personal, que anteriorment he esmentat, en relació l'ús i el control del correu electrònic en l'àmbit laboral, tals com el Grup de Treball de l'article 29, que interpreta la Directiva Europea 95/46/CE, l'Agència Espanyola de Protecció de Dades, en endavant AEPD, i l'Autoritat Catalana de Protecció de Dades, en endavant APDCAT.

3.1.1. EL GRUP DE L'ARTICLE 29

En relació el criteri del GT 29 sobre l'ús del correu electrònic en l'àmbit laboral, cal destacar el **Document de Treball relatiu a la vigilància de les comunicacions electròniques en el lloc de treball** que va aprovar en data 29 de maig de 2002, ja que analitza la vigilància que l'empresari pot establir sobre la utilització del correu electrònic per part dels treballadors.

[5] ***Marín Alonso, Inmaculada:*** *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones. Editorial Tirant lo Blanch. València (2005).*

Així, els missatges de correu electrònic han de beneficiar-se de la mateixa protecció que els missatges de correu ordinari. En aquest sentit, el GT 29 considera que la prevenció hauria de prevaler davant la detecció, és a dir, l'empresari hauria de prevenir la utilització massiva del correu electrònic abans que detectar que certs treballadors en fan un ús incorrecte.

El GT 29 considera essencial que l'empresari informi als seus treballadors sobre la presència, utilització i objectius de tots els equips de treball, entre ells l'ordinador, així com de qualsevol abús detectat en els mateixos, mitjançant finestretes d'advertència, per exemple, on cada treballador pugui veure constantment el procés que l'empresari segueix en l'exercici de la seva facultat de vigilància i control en l'empresa. Així mateix, l'empresari podria proporcionar a cada treballador dos comptes de correu electrònic; Un d'ús estrictament professional que es podria controlar amb els límits establerts en el document de treball i l'altre d'ús privat el qual es controlaria únicament en casos de seguretat. D'aquesta manera, es reduiria el risc d'intromissió a la vida privada dels treballadors. A més a més, això permetria controlar a l'empresari en quina mesura utilitza el treballador l'ús del correu electrònic comptabilitzant el temps que inverteix en el correu personal i quin temps inverteix en el correu professional.

Ara bé, no podem deixar de banda destacar que, tal i com així ho indica el GT 29 en el document de treball analitzat, si l'empresari vol establir un control legal i justificable sobre l'ús del correu electrònic ha de fer-ho basant-se amb els següents principis:

- Necessitat: Abans que l'empresari procedeixi a la vigilància de l'ús del correu electrònic per part del treballador, aquest haurà de valorar si aquesta vigilància és absolutament necessària. En aquest sentit, serà necessària quan es vulgui confirmar o comprovar determinats actes del treballador o quan sigui necessària pel bon funcionament del sistema (seguretat, detecció de virus...).
- Finalitat: Les dades que s'obtenen amb el control de l'ús del correu electrònic han de recollir-se amb fins determinats, explícits i legítims, i no ser tractades posteriorment de manera incompatible.

- Transparència: L'empresari mai podrà realitzar un control secret sobre el correu electrònic del treballador ja que està obligat a indicar de forma clara i obertament les seves activitats, excepte en aquells estats membres on una llei preveu el contrari. Així, s'haurà de proporcionar al treballador informació clara i precisa relativa a la vigilància del correu electrònic, s'haurà de notificar a les autoritats de supervisió i s'haurà de garantir el dret a l'accés per part del treballador a les dades personals i als arxius de l'empresari.
- Legitimitat: Es controlarà l'ús del correu electrònic per part de l'empresari quan sigui necessari per satisfer un interès legítim, per exemple, quan aquest vulgui defensar la seva empresa d'amenaces.
- Proporcionalitat: Tota dada personal ha de ser adequada, pertinent i no excessiva en relació al fi per la qual s'obté. Per exemple, només es podria controlar l'ús del correu electrònic si resulta necessari per garantir la seguretat del sistema.
- Exactitud i conservació de les dades: Les dades que s'obtinguin a través del control de l'empresari sobre l'ús del correu electrònic hauran de ser precises i actualitzar-se ja que no poden conservar-se durant molt temps.
- Seguretat: L'empresari haurà de garantir l'aplicació de mesures tècniques i organitzatives per tal de vetllar per la protecció de les dades de caràcter personal de cara a tercers. Per tant, el control de l'ús del correu electrònic no ha de considerar-se una violació del dret del treballador a la vida privada sempre i quan hi hagin garanties.

En definitiva, el control de l'empresari sobre l'ús del correu electrònic per part del treballador només es justificarà en circumstàncies limitades ja que per accedir-hi és necessari un interès legítim per part de l'empresari. De no ser així, preval el dret fonamental al secret de la correspondència de l'article 18.3 de la CE.

3.1.2. L'AGÈNCIA ESPANYOLA DE PROTECCIÓ DE DADES

En matèria de telecomunicacions, l'AEPD s'encarrega de tutelar els drets i garanties dels usuraris en l'àmbit de les comunicacions electròniques. En aquest sentit, doncs, s'encarrega de controlar l'ús del correu electrònic en les empreses per tal d'enviar comunicacions comercials.

Un dels informes de l'AEPD que cal destacar, és **l'informe 0247/2008 relatiu a l'accés de l'empresari sobre l'ús del correu electrònic per part dels treballadors**. En aquest informe, l'Agència estableix que existeix legitimació per a que l'empresari pugui accedir a controlar l'ús i els continguts dels correus electrònics dels treballadors, en virtut de l'article 6.2 de la LOPD i de l'article 20.3 de l'Estatut dels Treballadors. No obstant, aquest accés només es permetrà en aquells casos que el correu electrònic hagi estat proporcionat per l'empresa per tal de complir amb les funcions laborals i sempre que prèviament l'empresa hagi advertit de tal control als treballadors, complint així amb el dret d'informació establert a l'article 5.1 de la LOPD. Per tant, els treballadors seran informats sobre els motius pels quals es realitzarà aquesta vigilància sobre l'ús del correu electrònic, les dades que es poden recollir amb l'acció de la vigilància, les característiques de la tecnologia utilitzada, les persones a les que es poden comunicar aquestes dades i el seu dret a tenir accés a les dades processades. Tanmateix, s'estableix com a recomanació que els representants dels treballadors també siguin informats per tal de ser capaços en qualsevol moment de comprovar que es protegeix la intimitat dels treballadors.

A més a més, l'AEPD quan tracta temes referents a l'ús del correu electrònic en l'àmbit laboral es refereix al Grup de Berlin[6], i concretament en el seu **informe i recomanacions sobre les telecomunicacions i la privacitat en les relacions laborals** de l'any 1996.

---

[6] ***GRUP DE BERLIN:*** *Organització especialitzada en tecnologies de la informació del Comissionat de Protecció de Dades i Llibertats d'informació de Berlin, que supervisa el compliment de la legislació sobre la protecció de dades a l'Estat de Berlin i assegura el dret fonamental a l'autodeterminació informativa.*

Segons aquest informe l'Agència es pronuncia dient que les tecnologies de la informació i la comunicació han canviat al llarg dels anys i que actualment s'han multiplicat els mètodes per a la recollida de informació. Continua afirmant que aquest mètodes es duen a terme per raons de seguretat, per controlar i assignar els costos de les diferents actuacions i comunicacions i per mesurar i millorar la productivitat. Per tant, la contínua supervisió i la recollida de dades relatives als diferents aspectes de l'activitat del treballador, possiblement sense el seu coneixement, és factible.

L'informe del Grup de Berlin afirma que les noves tecnologies de la informació, com ara el correu electrònic, permeten la supervisió permanent i la vigilància del lloc de treball, i que en determinats casos la informació recollida pot ser utilitzada en secret o fins que els treballadors no en són conscients. Aquesta tecnologia, doncs, planteja greus amenaces d'intrusió en la privacitat de l'usuari. Per aquesta raó, es recomana a l'empresari que asseguri al treballador una zona en l'empresa on es garanteixi la seva privacitat, i permeti una lliure comunicació amb altres persones per rebre o enviar missatges personals.

3.1.3. L'AUTORITAT CATALANA DE PROTECCIÓ DE DADES

Respecte el pronunciament de l'APDCAT sobre l'ús del correu electrònic en l'empresa, cal destacar la **recomanació 1/2013 sobre l'ús del correu electrònic en l'àmbit laboral**. Amb aquesta recomanació l'Autoritat pretén establir unes pautes d'accés al correu electrònic per part de l'empresa ja que en els últims anys s'ha considerat una eina imprescindible en qualsevol centre.

En primer lloc, l'Autoritat deixa clar que qualsevol empresa ha d'establir i posar en coneixement als seus treballadors, i als representants dels mateixos, les normes d'ús del correu electrònic ja que una manca de política adequada d'ús del correu electrònic pot provocar una situació conflictiva per falta de confidencialitat.

L'APDCAT permet que les empreses facilitin als seus treballadors dos comptes de correu, d'acord amb la seva finalitat; Un compte corporatiu per a ús laboral que serà propietat de l'empresa i que determina l'usuari, el proveïdor i les condicions d'ús, i un compte corporatiu per a ús privat el qual podrà limitar-ne l'ús però no controlar-ne el contingut. Per tal d'abastar el control d'aquests comptes, l'empresa ha de limitar les dades sobre els emissors i els receptors, l'hora de connexió, el nombre de missatges enviats i els tipus d'arxius que s'adjuntin en cada correu electrònic. Ara bé, en cas que aquesta informació sigui escassa, l'empresari podrà accedir al control del contingut dels correus electrònics, evitant accedir a missatges privats. Aquest accés serà limitat en funció dels objectius de l'empresa, és a dir, l'empresari només podrà controlar l'ús dels correus electrònics en quatre situacions:

- Quan s'hagin de realitzar tasques de manteniment, de suport tècnic o de la seguretat del sistema del correu electrònic. Aquestes tasques únicament podrà dur-les a terme personal autoritzat pel responsable de seguretat.
- Quan sigui necessari per garantir la continuïtat de l'activitat en absència de la persona treballadora, ja que una absència de llarga durada provoca problemes en l'activitat normal de l'empresa si no es pot accedir a un determinat compte de correu electrònic.
- Quan hi hagi indicis d'un possible mal ús, sempre que l'accés sigui proporcionat al tipus de risc que es pugui derivar del mal ús del correu electrònic.
- Quan es produeixi un cessament de la relació laboral del treballador, ja que s'haurà de inhabilitar els codis d'usuari i les contrasenyes. Els missatges personals que constin en el compte de correu corporatiu s'hauran de facilitar al treballador, i en cas de defunció es podran eliminar.

3.2. NORMES RELATIVES A L'ÚS DEL CORREU ELECTRÒNIC EN L'EMPRESA

En aquest apartat vull aprofitar la visita que vaig fer el dia quatre d'abril de dos mil catorze (04/04/2014) a una empresa[7] formada per experts en assessorament en l'àmbit de protecció de dades en empreses, per destacar qüestions més pràctiques que em van explicar sobre la normativa i condicions d'ús del correu electrònic en les empreses.

En un primer moment vàrem destacar l'article 4 de la LOPD referent a la qualitat de les dades. Sabem que aquestes han de ser les justes i necessàries per tal de que puguin ser tractades, i que en cap cas es poden recopilar de forma fraudulent o il·lícita.

En un segon lloc vàrem parlar sobre la política d'enviament de correus electrònics en l'empresa, és a dir, sobre aquells conceptes o normes bàsiques que qualsevol empleat ha de conèixer sobre la seva empresa. Per tant, és molt important deixar clar que els treballadors han de conèixer la LOPD ja que no poden enviar dades personals sense mesures de seguretat. Algunes d'aquestes mesures són les següents:

1. El contingut dels correus electrònics ha d'enviar-se de forma encriptada o protegida. Pel que fa la diferència entre dades encriptades o protegides és que si enviem un correu encriptat únicament el seu destinatari en podrà veure el contingut i si enviem un correu protegit es requerirà una clau per part del destinatari per tal de poder-hi accedir.
2. Per enviar correus electrònics publicitaris sobre l'empresa es requereix primerament un consentiment del seu destinatari (article 21 de la llei 34/2002, de 11 de juliol, de serveis de la societat de la informació i del comerç electrònic). Així doncs, quan els treballadors d'una determinada empresa hagin d'enviar correus electrònics publicitaris hauran de sol·licitar una autorització a cada destinatari.

[7] ***Pedrosa Busquets & associats:*** *Empresa d'assessorament en protecció de dades en les empreses de Tona (Barcelona).*

Ara bé hi ha una excepció a aquesta regla, i és que no es requerirà aquest consentiment quan existeixi una relació contractual entre l'empresa i el destinatari del correu electrònic, és a dir, els treballadors podran enviar correus publicitaris als clients de l'empresa, als seus proveïdors... En cas d'incomplir amb aquesta regla, l'empresa hauria comès una falta greu i li correspondria com a tal una multa de 30.000 a 300.000 euros.

3. Quan una empresa envia correus electrònics, ja sigui als seus clients o proveïdors, amb fitxers adjunts tals com nòmines o factures, sempre haurà de posar tots els seus destinataris ocults ja que aquests no poden veure els comptes de correu electrònic els quals se'ls ha enviat el mateix correu.

Finalment, vàrem destacar que una bona política d'empresa és aquella que deixar clar quines són les normes d'ús del correu electrònic, i sobretot quines són les mesures de vigilància que aplicarà l'empresa per tal d'establir-ne un control. A més a més, una política d'aquest caire hauria d'establir quin és el període de temps que l'empresa considera necessari per mantenir un correu electrònic a la safata d'entrada, ja que cap llei en fa especial referència.

Per últim, destacar que per acabar de tenir una bona política d'empresa sobre les condicions d'ús del correu electrònic, l'empresa hauria de facilitar, juntament amb el compte de correu electrònic proporcionat al treballador, una clau personal d'accés al mateix intransferible que es renovés periòdicament per tal d'evitar-ne qualsevol tipus de plagi.

3.3. ANÀLISI DE LA JURISPRUDÈNCIA RELATIVA AL CORREU ELECTRÒNIC

En aquest apartat, analitzaré com s'han manifestat diversos Tribunals dels nostre ordenament jurídic respecte l'ús i control empresarial del correu electrònic en les empreses. Per això, s'haurà de tenir present els criteris establerts pels propis organismes de protecció de dades, tals com el GT 29, l'AEPD i l'APDCAT, en els seus informes o dictàmens.

3.3.1. SENTÈNCIES DE DIFERENTS ÒRGANS JUDICIALS

En primer lloc, vull fer referència a la **Sentència del Tribunal Superior de Justícia de Catalunya 9382/2000, de 14 de novembre**. Aquesta sentència tracta sobre un treballador que és acomiadat disciplinàriament pel fet d'utilitzar el correu electrònic que l'empresa l'hi ha proporcionat amb fins personals, sense coneixement ni autorització. L'empresa al·lega que procedeix a acomiadar al treballador ja que ha tingut coneixement de que tal treballador ha enviat una gran quantitat de correus electrònics amb missatges humorístics i sexistes als seus companys de treball, en horari laboral. En virtut d'allò establert en l'informe 0247/2008 relatiu a l'accés de l'empresari sobre l'ús del correu electrònic per part dels treballadors de l'AEPD, l'empresa pot accedir al contingut dels missatges de correu electrònic que envien els treballadors sempre i quant aquest s'hagi proporcionat per servir l'activitat laboral de l'empresa. És per aquesta raó, que l'empresa, en virtut del Conveni Col·lectiu d'aplicació i de l'Estatut dels Treballadors decideix acomiadar al treballador. Respecte la decisió del TSJC sobre el tema, aquest al·lega que es dóna una transgressió de la bona fe contractual i abús de la confiança (article 5 de l'ET) i per tant declara l'acomiadament com a procedent ja que el treballador ha incomplert els seus deures de conducta i compliment establerts al contracte de treball.

Seguint amb la sentència número 9382/2000 del TSJC, l'empresa fa constar com a fet provat que segons la seva política d'empresa només permet la utilització del correu electrònic, tant per rebre com per enviar missatges, per motius de treball. Aquest fet és totalment acord a la recomanació 1/2013 sobre l'ús del correu electrònic en l'àmbit laboral de l'APDCAT quan estableix que qualsevol empresa hauria de tenir una política sobre les normes d'ús dels mitjans de comunicació electrònics. A més a més, el TSJC ha procedit a declarar procedent l'acomiadament ja que el control empresarial relatiu a l'ús del correu electrònic que l'hi ha donat peu, s'ajusta a tots els principis exposats pel GT 29 en el seu Document de Treball relatiu a la vigilància de les comunicacions electròniques en el lloc de treball de 2002.

Un altre fet a destacar és que el Tribunal no ha considerat l'acomiadament com a nul ja que sustenta que perquè un acomiadament sigui nul s'ha de vulnerar un dret fonamental, i en aquest cas, el dret fonamental a la protecció de dades no és vulnera ja que el control que estableix l'empresari sobre els missatges de correu electrònic del treballador està justificat i degudament acreditat. D'altra banda, el Tribunal declara la inexistència de discriminació cap al treballador acomiadat, i per tant, tampoc es podria considerar un acomiadament nul.

Una altra sentència referent a l'ús del correu electrònic en l'empresa és la **STSJ de Madrid 393/2001 de 12 de juny**. En aquest cas, el Tribunal ha optat per considerar que un treballador ha estat acomiadat improcedentment pel fet d'utilitzar el correu electrònic en el seu lloc de treball de manera personal, és a dir, per fins personals. Aquesta sentència resulta similar, però alhora contrària, a la sentència esmentada anteriorment i per aquesta raó, és interessant veure'n els fonaments jurídics en que es base el Tribunal, sabent que aquest és de la mateixa categoria.

Així doncs, en aquest cas, el Tribunal Superior de Justícia de Madrid, en endavant TSJM, manifesta que tot i que el treballador utilitzi el correu electrònic per fins personals, no li correspon la falta més greu tipificada en el seu Conveni Col·lectiu d'aplicació, i per tant qualifica l'acomiadament com a improcedent.

Cal destacar que en base la recomanació 1/2013 sobre l'ús del correu electrònic en l'àmbit laboral de l'APDCAT, l'empresari ha accedit correctament al control de l'ús del correu electrònic en l'empresa ja que aquest hi ha accedit per indicis d'un possible mal ús. En efecte, l'empresa ha tingut coneixement de que el treballador va enviar correus electrònics amb contingut pornogràfic, tot i que segons l'hora d'enviament consta que els va enviar durant la seva hora lliure, hora que disposa per dinar.

Tant el Tribunal com l'empresa no fan constar que l'empresa tingués cap normativa d'ús del correu electrònic, ja que no s'expressa que aquesta última limités el número de missatges de correu als treballadors, les hores de connexió, o fins i tot el tipus de fitxers, tant quantitatiu com qualitatiu, adjunts a tals correus. En aquest sentit, doncs, no es segueix la recomanació 1/2013

sobre l'ús del correu electrònic en l'àmbit laboral de l'APDCAT. Ara bé, el que si que es posa en manifest és que l'empresa disposa d'un sistema de seguretat informàtica en que cada treballador té diferents claus d'accés als ordinadors, i per aquesta raó resulta evident afirmar que el treballador és l'únic subjecte responsable del contingut dels correus electrònics enviats amb fins personals.

Una altra sentència rellevant sobre l'ús del correu electrònic en l'empresa que m'agradaria destacar és la **Sentència de l'Audiència Nacional 13/2014, de 28 de gener.** En aquesta sentència es tracta el tema de que una empresa estableix una clàusula en els contractes de treball dels treballadors, en que obliga a aquests a facilitar el seu correu electrònic i el seu telèfon mòbil a l'empresa per tal de que aquesta pugui comunica'ls-hi qualsevol tema referent a la seva activitat laboral.

La Sala Social de l'Audiència Nacional, en endavant SSAN, en virtut de l'article 3.A de la LOPS, ha considerat que les dades relatives al telèfon mòbil o al correu electrònic són dades de caràcter personal, i que per tant, seran protegides com a tal. En aquest sentit, i conforme l'article 6 de la citada llei, qualsevol tractament de dada personal requereix el consentiment de l'afectat. No obstant, en aquells casos en que no és necessari tal consentiment, l'afectat podrà oposar-se al seu tractament si es donen motius fonamentals relatius a una situació personal concreta.

En definitiva, la SSAN manifesta que la clàusula que l'empresa estableix als contractes de treball és abusiva i per tant en declara la seva nul·litat, ja que considera que les dades relatives al correu electrònic i al telèfon mòbil requereixen el consentiment de l'interessat i en cap cas poden ser objecte d'una clàusula pel fet que provoca un desequilibri de drets i obligacions i un perjudici desproporcionat i no equitatiu. Ara bé, la SSAN també afegeix que de forma voluntària, els treballadors podran facilitar les dades personals que considerin oportunes a l'empresa.

En aquest sentit, doncs, no es compleixen els principis establerts pel GT 29 en el seu Document de Treball relatiu a la vigilància de les comunicacions electròniques en el lloc de treball de 2002, ja que el fet que l'empresa vulgui imposar com a clàusula que els treballadors li facilitin dades personals no es

considera ni necessari, ni legítim ni proporcional. En tot cas, aquesta empresa el que hauria de fer és seguir la recomanació 1/2013 sobre l'ús del correu electrònic en l'àmbit laboral de l'APDCAT i proporcionar a cada treballador de la seva empresa un compte corporatiu de correu electrònic amb finalitat laboral, per poder comunicar-se amb cada treballador sobre qüestions estrictament professionals, i així mantenir-se al marge de la seva intimitat i sobretot de la seva vida privada.

Respecte el pronunciament del Tribunal Suprem, en endavant TS, considero oportú destacar la **Sentència del Tribunal Suprem 7514/2007, de 26 de setembre.** Aquesta sentència resulta interessant ja que dóna resposta a un recurs de cassació per a la unificació de la doctrina que planteja la compatibilitat del control empresarial amb el dret fonamental dels treballadors a la seva intimitat, al secret de les comunicacions i a la protecció de dades personals. En aquest cas no es tracta de valorar la conducta del treballador a efectes disciplinaris, sinó de limitar el control empresarial sobre el registre d'objectes personals del treballador establert a l'article 18 de l'Estatut dels Treballadors.

El recurs estableix que un treballador va ser acomiadat ja que l'empresa, en plena pràctica d'anàlisi i reparació informàtica de l'ordinador del treballador a efectes de controlar-ne el funcionament del sistema, va descobrir que l'ordinador tenia virus informàtics pel mal ús que el treballador en feia, és a dir, per la navegació en pàgines poc protegides a Internet. En aquest sentit, el Tribunal considera "*que el control dels ordinadors, o fins i tot del correu electrònic, és justifica per la necessitat de coordinar i garantitzar la continuïtat de l'activitat laboral i per la protecció del sistema informàtic de l'empresa, que pot veure's afectat negativament per determinats usos, i per la prevenció de responsabilitats que l'empresa pugui tenir derivada de formes il·lícites d'ús davant a tercers.*" Per aquesta raó, s'entén que el control que estableix l'empresari davant els mitjans de treballs que facilita als treballadors no necessita justificació, al contrari del que estableix l'article 18 de l'Estatut dels Treballadors quan considera que només es realitzaran registres en les taquilles i efectes particulars dels treballadors. Així, està clar que l'empresari ha de controlar l'ús i els continguts de l'ordinador ja que amb ell es compleix la prestació laboral.

Ara bé, cal tenir en compte que durant el registre de l'ordinador del treballador, no va ser-hi present ni el propi treballador ni un representant del mateix, a més de que posteriorment l'ordinador va ser traslladat a la botiga de reparacions, interpretant-se tal fet com un control de l'ordinador fora del lloc i l'horari de treball. Per tant, ens podríem trobar davant una inaplicació de l'article 18 de l'Estatut dels Treballadors. En aquest sentit, però, l'article 18 de l'Estatut dels Treballadors es refereix al registre de taquilles i efectes particulars del treballador i per tant, el correu electrònic no es podria considerar un efecte particular del treballador pel fet de que aquest és considerat una eina de treball.

En síntesis, d'acord amb la STS, l'empresa no pot controlar ni espiar l'ús que els treballadors fan de l'ordinador o el correu electrònic ja que de ser així es vulnera el dret a la intimitat. No obstant, si que adverteix que l'empresari té potestat per controlar altres mitjans laborals. Per això, l'empresa hauria d'establir prèviament normes d'us d'aquests medis, a través d'una política d'empresa, amb prohibicions totals o parcials i comunicar als treballadors de que es realitzarà un control sobre els mateixos. Per tant, l'empresa ha d'informar als treballadors que posa a la seva disposició un ordinador o un compte de correu electrònic únicament per fins laborals i que no es tracta en cap cas d'un compte personal, evitant així que aquest enviï comunicacions personals.

Com a última sentència relativa a l'àmbit de les comunicacions electròniques en el centre de treball, vull destacar la **Sentència del Tribunal Europeu de Drets Humans, de 3 d'abril de 2007 sobre el famós Cas Copland.** En aquest cas, no es tracta únicament l'ús del correu electrònic, sinó que la demandant al·lega que ha tingut coneixement de que l'empresa per la qual treballa ha interceptat durant diversos mesos informació sobre la utilització personal del seu correu electrònic, les trucades rebudes i enviades i la navegació per Internet.

En aquest sentit, es planteja que es produeix una violació de l'article 8 del Conveni Europeu de Drets Humans, en endavant CEDH, ja que es considera que el correu electrònic és un instrument protegit per tal article: *" **1.** Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y*

de su correspondencia. ***2.*** *No podrà haver injerencia de la autoridad pública en el ejecricio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la Ley y ocnstituya una medida que, en una sociedad democràtica, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás ".* Aquest article deixa clar que qualsevol persona té dret a que se li respecti la seva vida privada, fins i tot en l'àmbit laboral, i que únicament es podrà interferir en ella quan sigui per raons estrictament necessàries. Per aquesta raó, en el Cas Copland s'estaria violant aquest dret reconegut ja que l'empresa s'interposa en la vida privada de la demandat per la simple raó de controlar que utilitzi adequadament els instruments electrònics que l'empresa li proporciona, és a dir, que no els utilitzi de forma personal.

Pel que fa la part contrària, es defensa al·legant que en cap moment ha interceptat el contingut dels correus electrònics, de les pàgines web visitades o de les trucades telefòniques, sinó que únicament n'ha establert un seguiment i que per aquesta raó no es podria considerar que el control sobre la demandant interfereixi en la seva vida privada, ja que es realitzava en virtut de protegir els drets i llibertats de la resta de treballadors i assegurar que no s'abusés de les instal·lacions de l'entitat pública.

Ara bé, no obstant lo exposat per la part contraria, el Tribunal Europeu de Drets Humans, en endavant TEDH, considera que la recollida i el tractament de la informació personal relativa a les trucades, als correus electrònics i a la navegació per Internet sense consentiment de l'afectada constitueix una violació al dret a la vida privada en el centre de treball, i que per tant, efectivament es produeix una violació de l'article 8 del CEDH. A més a més, el Tribunal no té coneixement de que l'empresa disposi d'una normativa interna que reguli les circumstàncies en que es pot realitzar un seguiment de l'ús del telèfon, del correu electrònic o de la navegació per Internet. Per tant, en tot cas l'empresa hauria d'intentar establir unes normes d'ús sobre tals instruments i mantenir als treballadors al corrent de les mateixes, a més d'advertir en tot moment que es podrien realitzar controls puntuals per assegurar el seu compliment. Així doncs, una vegada més ens trobem davant la necessitat

reconeguda per l'APDCAT en la seva recomanació 1/2013 sobre l'ús del correu electrònic en l'àmbit laboral, d'establir una política d'empresa relativa a l'ús del correu electrònic

3.3.2. LA STC 170/2013 DE 7 D'OCTUBRE

Degut a la importància que té la Sentència del Tribunal Constitucional, en endavant STC, 170/2013 de 7 d'octubre, i lo recent que és, analitzaré amb més detall els fonaments jurídics de la mateixa per tal d'extreure'n conclusions rellevants sobre la utilització de les comunicacions electròniques en el centre de treball.

En primer lloc cal resumir breument quina és la controvèrsia en que es troba el TC. Així doncs, amb aquesta sentència el TC pretén analitzar si la sentència del TSJM de 27 d'abril de 2013 impugnada per la part demandant del procés, en aquest cas un treballador, vulnera els drets fonamentals de la intimitat i el secret de les comunicacions del mateix ja que s'ha considerat com a lícita, en el procés d'acomiadament del treballador, una prova presentada per l'empresa on hi constava el contingut de diferents correus electrònics reveladors de informació i secrets professionals de l'empresa i enviats pel demandant. A més, tal i com s'especifica, aquests correus electrònics s'han obtingut mitjançant l'accés a l'ordinador del treballador, ordinador propietat de l'empresa. Per la seva importància, cal destacar també que el Conveni Col·lectiu d'aplicació sanciona com a falta lleu la utilització dels mitjans informàtics propietat de l'empresa per usos diferents als relacionats amb la prestació laboral.

Inicialment el TC parteix de l'article 20 de l'Estatut dels Treballadors el qual atorga potestat a l'empresari per adoptar les mesures que consideri necessàries per tal de vigilar i controlar el compliment de les obligacions laborals dels treballadors. El TC estableix que en virtut d'aquest article no es podria considerar que es vulneren els drets fonamentals al·legats pel treballador ja que afirma que els correus electrònics en l'àmbit laboral són

instruments que no queden protegits per l'article 18 de la CE pel fet de que s'envien a través d'un canal el qual no es pot garantir la seva confidencialitat, és a dir, el considera un canal de comunicació oberta a la inspecció empresarial, i pel fet de que no es considera un efecte personal del treballador, sinó una eina de treball.

A més, amb la sentència dictamina que a l'empresa existia una prohibició expressa tipificada al Conveni Col·lectiu d'aplicació sobre l'ús personal dels mitjans informàtics proporcionats per l'empresa, i que per tant com a norma de caràcter vinculant, no es podia garantir la confidencialitat de tot allò que quedés registrat als ordinadors i de les converses mantingudes pels treballadors a través del correu electrònic. És per aquesta raó que en aquest cas es podria interpretar que la prohibició de l'ús extra laboral del correu electrònic porta implícita la potestat de l'empresari de controlar la seva utilització per tal de verificar el compliment del treballador de les seves obligacions laborals.

Un fet important a destacar és que el treballador al·lega que mai ha tingut coneixement de que l'empresa disposés d'una política referent als límits i condicions sobre la utilització dels ordinadors i el correu electrònic en l'empresa, així com tampoc ha tingut coneixement d'aquells procediments a seguir per tal de controlar-ne el seu contingut. En aquest sentit, el TC manifesta que aquest fet és contrari a les exigències de la doctrina del TS en la seva sentència de 26 de setembre de 2007, quan aquest es pronuncia dient que es produeix una vulneració al dret al secret de les comunicacions per no existir una prohibició absoluta i vàlida, ni cap advertència del control sobre l'ús de l'ordinador per fins personals. No obstant això, el TC també manifesta que el fet de que en el Conveni Col·lectiu d'aplicació s'hi tipifiqui com a falta lleu la utilització de mitjans informàtics proporcionats per l'empresa per fins personals, supleix la manca de política referent a l'ús d'aquests instruments en el treball, i considera que en cap moment s'està vulnerant el dret fonamental al secret de les comunicacions (article 18.3 CE).

Per tant, ens trobem davant un criteri jurisprudencial diferent als que ens trobàvem fins ara, ja que el TC permet a les empreses no tenir una política

sobre l'ús del correu electrònic sempre i quan en el Conveni Col·lectiu d'aplicació hi consti una falta disciplinària relativa a la utilització de tal instrument, a efectes de ser conegut i vinculant pel treballador. No obstant això, és deure de l'empresari establir límits sobre l'ús del correu electrònic, havent de definir si permet l'ús personal o no d'aquest per a que els treballadors actuïn seguint una política d'empresa.

Respecte l'aprovació de la prova documental relativa al contingut dels correus electrònics en el procés d'acomiadament del treballador, aquest sol·licita la nul·litat de la mateixa perquè considera que el contingut dels correus electrònics constitueix una prova il·lícita per la forma en que s'ha obtingut ja que l'empresari s'ha extralimitat en l'exercici de la seva potestat de vigilància i control per haver interceptat de forma il·lícita el mateix. Per tant, al·lega que en l'obtenció de la prova, és a dir en el registre i accés a l'ordinador del treballador, no s'han seguit els criteris doctrinals de la STS de 26 de setembre de 2007 que estableix determinats límits per registrar l'ordinador proporcionat al treballador per l'empresari. Ara bé, el TC entén que el control i vigilància que estableix l'empresari sobre els correus electrònics és idoni, necessari i proporcional, principis claus dictats pel GT 29 en el seu Document de Treball relatiu a la vigilància de les comunicacions electròniques en el lloc de treball de 2002, i per tant opta per considera que no es vulnera el dret fonamental a la intimitat (article 18.1 CE) rebutjant així la petició del treballador, i justificant-ho en base el judici de proporcionalitat. Per tant, recorda que per comprovar si una mesura restrictiva de dret fonamental supera el judici de proporcionalitat és necessari, com ja he dit anteriorment, verificar si compleix amb els tres requisits essencials:

1. Judici de idoneïtat: Si tal mesura és susceptible d'aconseguir l'objectiu que es proposa l'empresari.
2. Judici de necessitat: Si tal mesura és necessària, en el sentit de que no hi ha cap altra mesura per tal d'aconseguir l'objectiu proposat amb igual eficàcia.

3. Judici de proporcionalitat en sentit estricte: Si tal mesura és equilibrada ja que d'ella se'n deriven més beneficis per l'interès general que perjudicis.

En aquest sentit, el TC afirma que l'accés als correus electrònics per part de l'empresa reuneix tots els requisits i ho justifica de la següent manera:

- En primer lloc considera que l'accés al contingut dels correus electrònics és una mesura justificada ja que segons la sentència d'instància, es dur a terme per les sospites que l'empresa tenia sobre un comportament irregular del treballador. Aquest primer punt quedaria justificat pel criteri establert en la seva recomanació 1/2013 sobre l'ús del correu electrònic en l'àmbit laboral de l'APDCAT.
- En segon lloc considera que també és una mesura idònia per verificar si el treballador està utilitzant el correu electrònic de l'empresa per enviar missatges a tercers reveladors de dades confidencials de l'empresa, i per adoptar les mesures disciplinàries que convinguin.
- En tercer lloc considera que és una mesura necessària ja que el contingut dels correus electrònics serveix com a prova davant la impugnació judicial de la sanció empresarial. Així, deixa clar que únicament resulta important com a prova documental el contingut de tals correus, no la identificació dels destinataris.
- Finalment considera que es tracta d'una mesura ponderada i equilibrada ja que s'ha establert com a garantia que el control empresarial s'ha realitzat a través de la intervenció d'un pèrit informàtic i davant un notari. A més a més, afirma que el contingut de tals correus electrònics en cap moment mostra aspectes de la vida personal i familiar del treballador tals com ideologia, creences o aficions, sinó únicament aspectes relatius a l'activitat empresarial. Aquest fet es justifica segons el criteri de l'AEPD en l'informe i recomanacions sobre les telecomunicacions i la privacitat en les relacions laborals de l'any 1996 del Grup de Berlin ja que per raons de seguretat i millora de la productivitat, es pot supervisar el correu electrònic dels treballadors i recollir les dades necessàries.

CONCLUSIONS

L'ús del correu electrònic en l'àmbit laboral genera una necessitat a totes les empreses d'establir una política interna sobre el seu adequat ús i funcionament, ja que un ús extralaboral produeix a l'empresari costos econòmics. Aquests costos solen ser més indirectes que directes pel fet de que es perd temps de treball efectiu i per tant, influeix en la prestació que el treballador ha d'oferir, a més de que pot provocar danys patrimonials, com per exemple ruptures o virus informàtics en els ordinadors.

Respecte l'ús extralaboral del correu electrònic, la doctrina i la jurisprudència tenen en consideració el número de missatges enviats i rebuts i la naturalesa del contingut dels missatges. En relació el número de missatges enviats i rebuts es considera que és manifestació de falta greu per justificar l'acomiadament enviar i rebre correus electrònics de forma massiva. En relació la naturalesa del contingut es considera falta greu els insults o ofenses a superiors jeràrquics en missatges enviats a clients, les imatges ofensives per els companys, els continguts pornogràfics...

D'altra banda, vistos els criteris dels diferents organismes encarregats de vetllar per la protecció de dades i tota la jurisprudència analitzada, cal destacar que majoritàriament, els Tribunals tenen en compte les discussions de les autoritats, encara que en alguns casos no les consideren. Per exemple, en la STSJ de Madrid 393/2001 de 12 de juny, el TS no té en consideració imposar a l'empresa la necessitat d'establir una política d'empresa referent a l'ús del correu electrònic, fet importantíssim establert per l'APDCAT.

Des d'un altre punt de vista, cal veure l'evolució que ha près el correu electrònic com a eina de treball. Degut al desenvolupament de la tecnologia de la informació en les últimes dècades, els empresaris han anat proporcionant cada vegada més als seus treballadors comptes de correu electrònic per tal de que aquests puguin satisfer la prestació laboral. Ara bé, tal com l'ús del correu electrònic en l'empresa s'ha potenciat en els darrers anys, indirectament també s'ha utilitzat de forma individual, és a dir, cada vegada són més els treballadors

que inconscientment utilitzen el seu compte de correu electrònic en horari laboral per ús estricament personal. És per aquest motiu que ja a l'any 2000, tal i com s'ha vist en la més anterior de totes les sentències analitzades, es donava la necessitat d'establir una política d'empresa relativa a l'ús i funcionament del correu electrònic en l'àmbit laboral.

Un altre tema sobre el qual cal reflexionar, degut a la novadora i criticada STC 170/2013 de 7 d'octubre, és la incorporació al Conveni Col·lectiu de protocols d'utilització del correu electrònic. En primer lloc s'ha de destacar que el Conveni Col·lectiu aborda moltes qüestions laborals i per això ha d'actualitzar-se periòdicament degut al ràpid avanç de les noves tecnologies, i s'ha de comprovar que respecti sempre els drets fonamentals. Per això, s'han de tenir en compte quatre elements:

1. El correu electrònic és considerat una eina de treball posada a disposició del treballador per part de l'empresa, i per tant està vinculat a un ús professional. En aquest sentit, no quedaria sota l'empara de l'article 18 de l'Estatut dels Treballadors ja que aquest es refereix únicament a taquilles o efectes personals dels treballadors.
2. L'empresari ha d'informar sobre les normes d'ús del correu al treballador ja que de no ser així es complicaria la seva potestat de vigilància i control pel fet de que es podria donar una vulneració dels drets fonamentals.
3. La informació sobre les condicions d'ús del correu ha de ser prèvia a l'inici de l'activitat laboral del treballador, no una vegada iniciada.
4. Han d'especificar-se mesures per tal d'evitar que un treballador pugui utilitzar lliurement i sense control el correu.

Per tant, tot i que el criteri jurisprudencial de la STC 170/2013 de 7 d'octubre ens indica que una prohibició expressa del correu electrònic en horari laboral en el Conveni Col·lectiu és substitutiva d'una política d'empresa, hem de ser conscients de que degut al desenvolupament tecnològic de les eines de treball actualment es requereix una regulació més específica sobre l'ús del correu electrònic en el treball, és a dir, el Conveni Col·lectiu no és suficient per regular-ne les seves condicions d'ús i funcionament. A més a més, cal deixar

clar que el contingut d'un Conveni Col·lectiu és molt extens i no sempre es té la certesa de que cada treballador se'l llegeixi, fet que fa que aquests no en coneixin realment les condicions. En aquest sentit, considero que no es compleix suficientment amb el dret a la informació, ja que amb el contingut d'un Conveni Col·lectiu passa el mateix que amb una política de privacitat: El fet de que sigui un contingut extens i dens fa que els usuaris no se'l llegeixen i per tant no en coneixin les condicions, a no ser que algú els en hi informi. Per tant, moltes vegades això ha fet que no es respecti el dret a la informació dels ciutadans.

En definitiva, les empreses es veuen obligades a establir una política que representi el seu compromís sobre les directrius a seguir respecte l'ús del correu electrònic en el treball i les mesures de vigilància que s'aplicaran al mateix. Ara bé, com ha de ser aquesta política?

En l'annex I del present treball es pot apreciar un model de política d'empresa proposada per l'APDCAT en la seva recomanació 1/2013. Aquest model es caracteritza per:

- Resulta apropiat per la direcció de l'empresa que l'elabori, ja que proporciona els elements i recursos suficients per el seu desenvolupament i implantació.
- És conforme a la legislació vigent aplicable i a altres possibles polítiques que tingui l'empresa.
- Defineix clarament als objectius marcats per l'empresa, així com les normes d'ús dels instruments de treball que seran objecte de vigilància i control.
- S'elabora en un llenguatge comprensible per cada treballador al que es dirigeix.

Tot i que el model de política proposat per l'APDCAT és correcta, considero oportú destacar que en aquest model, i en qualsevol altre, resulta imprescindible incorporar-hi cinc elements:

- Definir si el correu electrònic s'estableix com a via de comunicació interna en l'empresa, és a dir, entre els empleats en si o entre els empleats i la direcció.
- Definir quines són les mesures de vigilància que realitzarà l'empresari per tal de controlar-ne l'ús.
- Definir si el correu electrònic es permet utilitzar-se per ús personal o no. En el cas de que no es permeti, seria convenient deixar clar que només es permetrà per resoldre qüestions familiars urgents, sempre que no siguin abusives.
- Definir quin és el període de temps que s'ha de mantenir un correu electrònic a la safata d'entrada, ja que la llei no en fa referència.
- Definir la informació sobre la política de privacitat de forma clara i reiterada.

Per últim, referent a la política d'empresa sobre l'ús del correu electrònic i la seva vigilància, cal dir que aquesta ha d'actualitzar-se periòdicament quan així es requereixi per canvis en la situació regulada, per canvis legislatius, per canvis en el propi mitjà o per canvis en el col·lectiu d'empleats que seran sotmesos a tal política. En aquest sentit, és convenient que la direcció de l'empresa procedeixi a la consulta amb els representants dels treballadors per a que la política representi un consens entre la direcció i el col·lectiu de treballadors. A més, aquesta política ha de ser notificada i explicada personalment al col·lectiu de treballadors afectats, a més de que ha de formar part del pla de formació anual de l'empresa, i evidentment ha de posar-se a disposició de cada treballador afectat per a que aquest la pugui consultar de forma permanent. En síntesis, com ha esmentat anteriorment, aquesta política ha de posar-se en coneixement de cada treballador abans de que aquest inici la seva activitat laboral, ara bé, convé destacar que una vegada iniciada la relació laboral, l'empresari ha de continuar recordant als seus treballadors les condicions d'ús del correu electrònic i fer-les visibles en format paper per tal de penjar-les al tauló d'anuncis de l'empresa.

BIBLIOGRAFIA I FONTS

BIBLIOGRAFIA

- DESDENTADO BONETE, AURELIO Y MUÑOZ RUÍZ, ANA BELÉN. *Control informático, videovigilancia y protección de datos en el trabajo.* Editorial Lex Nova, mayo 2012.
- MARÍN ALONSO, INMACULADA. *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones.* Editorial Tirant lo Blanch, València 2005.
- MARZO PORTERA, ANA Y MARZO PORTERA, ICIAR. *Vigilancia y control de las comunicaciones electrónicas en el lugar de trabajo.* Editorial ediciones experiencia, SL, Barcelona 2009.
- ROIG BATALLA, ANTONI; GALA DURÁN, CAROLINA; MARTÍNEZ FONS, DANIEL Y MUÑOZ LORENTE, JOSÉ. *El uso laboral y sindical del correo electrónico e Internet en la empresa: Aspectos constitucionales, penales y laborales.* Editorial Tirant lo Blacn, València 2007.

BIBLIOGRAFIA WEB

- *Autoritat Catalana de Protecció de Dades.* Recomenació 1/2013 sobre l'ús del correu electrònic en l'àmbit laboral. Barcelona 2013. Disponible a http://www.apd.cat/ca/contingut.php?cont_id=83&cat_id=169 [Primera consulta: 05/03/2014]
- *Agència Espanyola de Protecció de Dades.* Informe 0247/2008 relatiu a l'accés de l'empresari sobre l'ús del correu electrònic per part dels treballadors. Madrid 2008. Disponible a http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2008-0247_Acceso-por-el-empresario-al-correo-electr-oo-nico-de-los-trabajadores.pdf [Primera consulta: 03/03/2014]

- *Agència Espanyola de Protecció de Dades.* Grup de treball de l'article 29: Document de Treball relatiu a la vigilància de les comunicacions electròniques en el lloc de treball. Publicació 29 de maig de 2002. Disponible a http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/2002/index-ides-idphp.php [Primera consulta: 20/02/2014]
- *Grup de Berlin.* Informe i recomanacions sobre les telecomunicacions i la privacitat en les relacions laborals. Berlin 1996. Disponible a http://www.datenschutz-berlin.de/ [Primera consulta: 12/02/2014]
- *Tribunal Constitucional.* Nota informativa 60/2013. Publicació 9 d'octubre de 2013. Disponible a http://icefconsultores.blogspot.com.es/2013/10/sentencia-sala-1-tribunal.html [Primera consulta 27/03/2014]

LEGISLACIÓ

- Espanya. Constitució Espanyola, de 6 de desembre de 1978. (BOE núm 311, de 29 de desembre de 1978).
- Directiva Europea 95/46/CE del Parlament Europeu, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques en lo que respecte el tractament de les dades personals i a la lliure circulació d'aquestes dades. (DOUE núm 281, de 23 de novembre de 1995, pàg 31-50).
- Conveni per la protecció dels Drets Humans i les Llibertats Fonamentals, Roma, 4 de novembre de 1950. (BOE núm 243, 10 d'octubre de 1979).
- Espanya. Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal. (BOE núm 298, de 14 de desembre de 1999).
- Espanya. Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions. (BOE núm 251, de 10 d'octubre de 2007).
- Catalunya. Llei 32/2010, de 1 d'octubre de 2010, de l'Autoritat Catalana de Protecció de Dades. (BOPC núm 804/VIII, de 4 d'octubre de 2010).

- Espanya. Reial Decret Legislatiu 1/1995, de 24 de març, pel que s'aprova el text refós de la Llei de l'Estatut dels Treballadors. (BOE núm 75, de 29 de març de 1995).
- Espanya. Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal. (BOE núm 17, de 19 de gener de 2008, pàg 4103-4136).

JURISPRUDÈNCIA

- Sentència del Tribunal Superior de Justícia de Catalunya 9382/2000 (Sala Social), de 14 de novembre (recurs 4854/2000).
- Sentència del Tribunal Superior de Justicia de Madrid 393/2001 (Sala Social, Secció 2na), de 12 de juny de 2001 (recurs 1207/2001).
- Sentència de l'Audiència Nacional 13/2014 (Sala Social, Secció 1a), de 28 de gener de 2014 (recurs 428/2013).
- Sentència del Tribunal Suprem 7514/2007 (Sala Social, Secció 1a), de 26 de setembre de 2007 (recurs 966/2006).
- Sentència del Tribunal Constitucional 170/2013, de 7 d'octubre de 2013.
- Sentència del Tribunal Europeu de Drets Humans, assumpte Copland contra el Regne Unit, de 3 d'abril de 2007.

ANNEX I: MODEL DE POLÍTICA D'EMPRESA SOBRE L'ÚS EL CORREU ELECTRÒNIC SEGONS L'AUTORITAT CATALANA DE PROTECCIÓ DE DADES

Normes d'ús del correu electrònic

1.- Objecte d'aquestes normes

..... *(nom de l'entitat)* assigna al personal que ho requereixi, per a l'exercici de les funcions que té encomanades, un equip informàtic i un compte de correu electrònic corporatiu mitjançant el sistema de client de correu .....

Aquest document té per objecte establir els criteris d'utilització del correu electrònic per al personal al servei de ..... *(nom de l'entitat)*, per garantir-ne un ús correcte.

2.- Instruccions generals d'ús del correu electrònic

El personal al servei de ..... *(nom de l'entitat)* ha de fer un bon ús del correu electrònic que li ha estat atribuït per a l'exercici de les seves funcions. Amb aquest objectiu, ha de complir aquestes normes.

Cada persona treballadora que té un compte de correu assignat es configura com a persona usuària d'aquests sistemes i és responsable d'aquests recursos que té assignats i de totes les accions que es duguin a terme en la seva utilització.

3.- Usos admesos del correu electrònic

L'ús del compte de correu electrònic facilitat per ..... *(nom de l'entitat)* s'ha de limitar al desenvolupament de les funcions pròpies del lloc de treball. D'acord amb això:

1. Només es pot emprar amb finalitats privades si es tracta d'un ús per motius personals o domèstics, que no sigui abusiu i no perjudiqui la seguretat dels sistemes d'informació de l'organització, ni el normal desenvolupament de les funcions encomanades.
2. No es pot utilitzar per a activitats professionals alienes a les tasques encomanades.

3. L'ús de comptes personals web mail només es pot fer per a finalitats personals amb les condicions exposades en el punt 3.1. En cap cas es pot emprar un compte de correu web mail per a l'exercici de les funcions encomanades, llevat que ho autoritzi .....
4. Les persones usuàries que tinguin atribuïda la gestió de comptes de correu genèrics associats a determinats tràmits o a unitats administratives (p. ex. consultes@.... .cat) en cap cas en poden fer un ús per motius personals, ni poden facilitar aquesta adreça amb finalitats personals.
5. No es permet l'ús del correu electrònic facilitat per contractar serveis personals no relacionats amb l'activitat professional.

Es prohibeix la configuració de comptes de client de correu als ordinadors de ..... *(nom de l'entitat)*, fora dels comptes facilitats per la mateixa entitat.
No es permet l'ús de programes xat, xarxes socials, missatgeria instantània, etc. durant la jornada laboral, llevat que estiguin vinculats a l'exercici de les funcions encomanades.

4.- Gestió de la bústia de correu

Correspon a cada usuari vetllar perquè la gestió de la informació continguda al seu correu electrònic sigui adequada. Per això:

1. Cal revisar i buidar periòdicament la safata d'entrada i, si escau, la de sortida, com a mínim, una vegada cada ... dies. Cal eliminar els missatges que no s'hagin de conservar i arxivar-ne la resta a la carpeta o subcarpeta adient, especialment els que poden tenir un contingut personal.
   Els missatges que formin part d'un procediment administratiu, o altres que s'hagin de conservar, només es poden eliminar del compte de correu si prèviament han estat degudament arxivats a l'expedient corresponent.
2. Els correus electrònics amb finalitats privades que es conservin s'han d'assenyalar com a tals, ja sigui mitjançant una denominació o marca que els permeti identificar, ja sigui mitjançant la creació d'una carpeta específica per a correus privats on es guardin aquest tipus de missatges.
3. Cal esborrar també, periòdicament, els missatges de la paperera o carpeta d'eliminats.

5.- Ús de les adreces publicades al directori de..... (nom de l'entitat)

Les adreces dels correus electrònics del personal al servei de ..... es publiquen a la intranet corporativa. Aquestes adreces es poden emprar:

a) Per a les comunicacions entre el personal vinculades a l'exercici de les funcions respectives .

b) Pels representants dels treballadors per trametre informació relacionada amb l'activitat sindical a l'empresa. Les persones treballadores poden oposar-se a la utilització de l'adreça amb aquesta finalitat, adreçant-se directament al sindicat que es tracti o bé a ....

En canvi, aquestes adreces no es poden facilitar a terceres persones alienes a l'organització, llevat que resulti necessari per a l'exercici d'alguna de les funcions encomanades.

Convé utilitzar el dret de cancel·lació davant terceres persones alienes a l'empresa que utilitzin indegudament la dada relativa a l'adreça de correu electrònic professional.

6.- Mesures de seguretat

6.1 Mesures generals

Les persones usuàries han de complir les mesures de seguretat següents:

a) Guardar l'usuari i la contrasenya d'accés al compte de correu de forma segura i no facilitar-los a altres persones, ni tan sols a efectes de manteniment del sistema.

b) No utilitzar una contrasenya fàcilment deduïble.

c) No fer ús de l'opció de guardar la contrasenya que s'ofereix a l'usuari per evitar reintroduir-la en cada connexió.

d) Bloquejar l'accés al compte de correu, en cas d'absentar-se del lloc de treball durant la jornada.

e) No seguir cadenes de missatges piramidals.

f) No desactivar els filtres de correu i les opcions de seguretat activades per l'administrador del sistema.

g) No utilitzar l'opció de vista prèvia.

h) No obrir missatges sospitosos. Comunicar-ho a ..... de forma immediata.

i) No enviar, reenviar o respondre missatges de correu que continguin dades sensibles, sense l'autorització de ..... .

j) En cas de detectar una incidència durant l'ús del correu electrònic, la persona treballadora ho ha de posar en coneixement del responsable de seguretat mitjançant ....., de forma immediata.

k) (*Altres* .....)

6.2 Signatura electrònica

Cal fer ús de la signatura electrònica quan sigui necessari per garantir l'autenticitat i la integritat del correu electrònic.

Es pot signar electrònicament un missatge amb el certificat electrònic facilitat per l'empresa, si es compleixen les dues condicions següents:

a) El correu s'envia associat a la identitat d'una persona. No és aplicable per tant, en casos de correus genèrics.

b) La comunicació s'efectua en exercici de les funcions atribuïdes. En queden exclosos, per tant, els correus personals o privats.

6.3 Missatges xifrats

Els missatges de correu electrònic s'han de xifrar quan continguin:

- Dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual.
- Dades obtingudes amb fins policials sense el consentiment de les persones afectades.
- Dades derivades d'actes de violència de gènere.
- Altres tipus de dades relatives a ...

7.- Altres normes de bon ús del correu electrònic

1. Emprar l'opció de còpia oculta (CCO), quan s'enviï un missatge a més d'una persona destinatària que no formi part de l'empresa.
2. Utilitzar l'opció de reenviar només en els casos en què la persona destinatària pugui accedir tant a l'emissor del missatge, com el seu contingut, i tota la informació de la cadena de correus que en formen part.
3. Eliminar el peu de signatura, si s'envia un missatge privat des del correu professional.
4. (*Altres*.....)

8.- Absència de la persona treballadora

En cas d'absència programada superior a ..... dies, es pot activar el missatge d'absència d'oficina per facilitar una altra adreça de contacte que garanteixi la continuïtat de l'activitat.

El text del missatge d'absència d'oficina serà el següent: "....."

Prèviament a l'absència, convé:

1. Guardar la informació personal o privada en una carpeta personal.
2. Transferir la informació necessària per continuar amb l'activitat durant l'absència.

9.- Cessament de la relació laboral

L'empresa pot cancel·lar la prestació del servei de correu en el moment en què finalitzi la relació contractual amb l'empleat o quan l'usuari n'estigui fent un mal ús.

La persona treballadora té dret a obtenir els missatges personals que en aquell moment estiguin emmagatzemats a la carpeta de missatges personals que designi o que es puguin identificar com a tals. La resta de missatges es poden analitzar per determinar si resulten necessaris per a la continuïtat de l'activitat o bé si es poden suprimir.

10.- Accés al correu electrònic fora del lloc de treball

Quan s'utilitzi el correu electrònic facilitat per l'empresa fora del lloc de treball cal tenir en compte:

a) No fer ús de l'opció de guardar la contrasenya, quan s'utilitzin ordinadors d'ús compartit.
b) Esborrar l'historial de navegació i tancar la sessió, en acabar, sempre que s'utilitzi un ordinador d'ús compartit per accedir al correu via web.
c) Utilitzar programes antivirus.
d) Utilitzar usuari i contrasenya per bloquejar els dispositius mòbils des d'on es pugui utilitzar el correu electrònic professional.
e) Emprar mecanismes de xifratge del contingut del dispositiu mòbil.

11.- Bones pràctiques en l'ús del correu

11.1 En relació amb els destinataris:

- Revisar les adreces dels destinataris, abans d'enviar el missatge.
- Valorar la utilització de l'opció de còpia oculta, per enviar un correu electrònic a múltiples destinataris.
- Quan es reenvia un correu electrònic, eliminar les adreces dels anteriors destinataris per no difondre, de forma injustificada, adreces de correu de tercers.

11.2 En relació amb l'assumpte:

- Identificar clarament i concisa l'assumpte.
- No incloure dades personals a l'assumpte.
- Evitar paraules o expressions que puguin activar els programes antiinundació *(antispam)*.

11.3 En relació amb el contingut:

- Revisar la possibilitat de revelar el contingut del missatge abans d'enviar-lo.
- Emprar el peu de signatura automàtic dels missatges de correu electrònic, d'acord amb el model corporatiu establert, que inclou la clàusula de confidencialitat. Quan es tracti de missatges amb finalitats personals, cal suprimir el peu de signatura.
- Organitzar els missatges enviats i rebuts en carpetes. Mantenir la safata d'entrada actualitzada.

11.4 En relació amb els arxius adjunts:

- Revisar la possibilitat de revelar el contingut dels arxius adjunts abans d'enviar-los.
- Evitar enviar arxius excessivament grans. El volum màxim previst és de ..... . Quan sigui superior, els arxius es poden comprimir.

12.- Accés al compte de correu electrònic per part de l'empresa

L'empresa pot fer controls automatitzats sobre l'ús del correu electrònic, per tal de vetllar pel normal funcionament del sistema (volum de trànsit, volum dels missatges enviats, etc.).

Només s'accedirà al contingut dels missatges o dels documents adjunts quan no es puguin utilitzar altres mecanismes menys intrusius, en els següents casos:

a) **Per dur a terme tasques de manteniment o vinculades a la seguretat del sistema**. En aquests casos, s'informarà la persona treballadora de les tasques que s'han de realitzar i se li oferirà la possibilitat de ser-hi present.

b) **Per comprovar, en el si d'una informació reservada o d'un procediment disciplinari, l'ús del correu electrònic, en aquells casos en què hi hagi indicis que la persona treballadora n'ha fet un mal ús**. En aquest cas, cal l'autorització del cap de recursos humans a petició de l'instructor del procediment. L'accés s'ha de fer en presència de la persona treballadora o, si escau, d'un representant del personal.

c) **Per garantir la continuïtat laboral en cas d'absència imprevista de la persona treballadora**. Si, per una necessitat improrrogable lligada a l'activitat laboral, cal accedir al contingut dels missatges del correu electrònic de la persona treballadora absent, aquesta pot delegar en una altra persona treballadora per verificar la forma com es duu a terme l'accés. No es pot accedir en cap cas, per aquest motiu, als missatges que la persona treballadora hagi assenyalat com a privats o que tingui emmagatzemats en una carpeta identificada com a privada.

13.- Conseqüències de l'incompliment d'aquestes normes d'ús del correu electrònic:

Quan l'empresa detecti que la persona treballadora fa un mal ús del correu electrònic que se li ha assignat, se l'advertirà formalment per escrit, sens perjudici de l'aplicació, si escau, del règim disciplinari corresponent.