

Dictamen en relació amb la consulta plantejada per la instructora d'un expedient disciplinari incoat a una funcionària d'un Ajuntament relatiu a l'ús privat del correu electrònic del lloc de treball

Es presenta davant l'Agència Catalana de Protecció de Dades un escrit de consulta emès per la instructora d'un procediment disciplinari incoat a una funcionària de l'administració local amb habilitació de caràcter estatal que ocupa el lloc de treball de Secretaria i Intervenció en un Ajuntament.

La instructora posa de manifest que la incoació de l'expedient disciplinari porta causa en un possible incompliment per part de dita funcionària local del deure de reserva professional pel que fa als assumptes que coneix per raó de les seves funcions, així com també en atenció al tractament de les dades de caràcter personal. La instructora formula una consulta a aquesta Agència "davant d'un possible cas de cessió o comunicació de dades de caràcter personal", i sol·licita a aquesta l'emissió d'un informe "respecte de l'expedient incoat en el seu dia".

I

(...)

II

Atès que la consulta té per objecte uns fets que han portat a la incoació d'un expedient disciplinari, esdevé rellevant fer un relat dels fets que es desprenen de la documentació aportada.

Mitjançant escrit de data 11 de novembre de 2009, l'alcalde de l'Ajuntament al qual pertany la funcionària local assenyala que en data 1 d'octubre de 2009 "com a conseqüència d'un procés de còpia de seguretat en compliment de les normes de seguretat, del tot rutinari com els realitzats amb anterioritat, es notifica una incidència, la qual comporta l'activació del protocol de seguretat i l'inici d'obtenció d'informació reservada per tal d'establir la certesa i l'abast dels fets observats en la incidència abans referenciada".

En data 1 d'octubre de 2009, l'administrador i responsable de seguretat del sistema implantat a l'Ajuntament comunica la incidència número 1/2009 al dit alcalde, el qual té la condició de responsable del fitxer. En l'apartat *incidència* de l'escrit de notificació, que és de tipus formulari, s'indica a que en data 1 d'octubre de 2009 l'operador de l'aplicació ha constatat en el moment de realitzar les còpies de seguretat que la carpeta d'elements enviats des de l'*Outlook* de Secretaria té un volum molt elevat en comparació amb la carpeta d'entrada, tenint en compte el curt període de temps (de 9/09/09 a 1/10/09), concretament té un volum superior a les 10 MB, i a l'apartat *efectes que pot produir* s'assenyala "un perill per a la seguretat de dades de caràcter personal".

En l'informe emès en data 1 d'octubre de 2009 per l'operador de l'aplicació encarregat d'administrar i mantenir l'estructura dels fitxers automatitzats de dades de caràcter personal d'aquest Ajuntament, s'assenyala el següent:

"Que en el dia d'avui, essent les divuit hores, en aplicació de la normativa de seguretat per a fitxers automatitzats de dades de caràcter personal amb nivell de seguretat

alt, a petició del responsable de seguretat de l'Ajuntament de xxx, s'efectua un control periòdic de verificació del compliment de les normes de seguretat, del tot rutinari com els realitzats amb anterioritat.

El control de verificació consisteix, com de costum, en primer lloc, en la revisió del servidor d'arxius i de les deu cintes de suport realitzades pel responsable de les còpies de seguretat. En segon lloc, es procedeix a la realització de les còpies de seguretat dels correus electrònics genèrics que es troben en funcionament a l'Ajuntament de xxx d'acord amb les prescripcions de l'Agència Catalana de Protecció de Dades.

D'aquest control de verificació de compliment es detecta una incidència que pot produir un perill per a la seguretat dels fitxers, entesa com la confidencialitat, la integritat i la disponibilitat de les dades."

Com a conseqüència de la comunicació d'aquesta incidència, en la mateixa data l'alcalde acorda l'obertura d'una Informació reservada per tal d'aclarir si la funcionària "ha pogut incomplir el deure de reserva professional pel que fa al tractament de dades protegides i als assumptes que coneix per raó de les funcions que li són encomandes".

Mitjançant escrit de data 16 d'octubre de 2009 signat per la mateixa funcionària local —tot i que l'expressió "rebut el 16-10-2009 a les 12,15 h" fa pensar que ha estat redactat pel mateix Ajuntament—, manifesta el següent:

"Jo....., declaro que sóc coneixedora del meu accés als Fitxers de dades personals:

<i>Nom dels fitxers</i>
<i>Outlook</i>
<i>Comptabilitat</i>
<i>Tributs i Taxes</i>

Per això, he rebut còpia de les meves Funcions i Obligacions sobre els citats Fitxers i declaro haver llegit i entès el que m'obliga, comproment-me a respectar, en la mesura que em pertoca segons el meu lloc de treball, el correcte compliment d'aquesta normativa.

També adquireixo el compromís d'utilitzar l'accés a la xarxa exterior (Internet) i al correu electrònic, proporcionat per l'Ajuntament per motius estrictament i exclusivament professionals, i en cap cas fer-ne un ús privat o particular. Així mateix autoritzo de forma informada i expressa a l'administrador del sistema a que revisi i inspeccioni els logs dels meus accessos a Internet com les direccions dels correus rebuts i enviats".

Pel que fa al contingut d'aquests fitxers, en l'Acord de creació de fitxers automatitzats que contenen dades de caràcter personal de l'Ajuntament s'indica el següent:

- El fitxer *Outlook* té per finalitat la gestió del correu electrònic de l'Ajuntament, obté dades personals del mateix personal de l'Ajuntament i de les persones que s'adrecen de forma presencial o telemàtica a l'Ajuntament, es recullen les dades següents: "Nom i cognoms i adreça del correu electrònic i aquelles altres exigides per la legislació vigent", no es preveuen fer cessions, l'òrgan responsable del fitxer és l'alcalde i té assignat un nivell bàsic de mesures de seguretat.
- El fitxer *Comptabilitat* té per finalitat la gestió comptable del pressupost i el registre de factures, obté dades personals dels proveïdors, de les persones que són deutores de l'Ajuntament i del personal de l'Ajuntament, es recullen les dades següents: "DNI/NIF/passaport, nom, cognoms, adreça, dades bancàries, telèfon i aquelles altres exigides per la legislació vigent", no es

preveuen fer cessions, l'òrgan responsable del fitxer és l'alcalde i té assignat un nivell bàsic de mesures de seguretat.

- El fitxer *Tributs i Taxes* té per finalitat la gestió i control de tots els tributs i taxes del consistori, obté dades personals de les persones que demanen els serveis recollits a les ordenances municipals de l'Ajuntament i dels contribuents, es recullen les dades següents: "Nom i cognoms i adreça del correu electrònic i aquelles altres exigides per la legislació vigent", no es preveuen fer cessions, l'òrgan responsable del fitxer és l'alcalde i té assignat un nivell mitjà de mesures de seguretat.

Com a part de la Informació reservada consten tres sol·licituds d'informació sobre dades de caràcter personal, totes de data 20 d'octubre de 2009 i amb subtítol "Exercici del dret d'accés (article 15 LOPD)", mitjançant les quals el representant legal de l'Ajuntament sol·licita –entendem que a l'encarregat del tractament ja que aquest sembla ser el dipositari del contingut dels fitxers– "que se li facilitin les seves dades de caràcter personal continguts en el fitxer indicat, així com la informació relacionada amb el tractament dels mateixos, de conformitat amb el dret d'accés regulat en l'article 15 de la Llei orgànica 15/1999". En l'apartat "nom del fitxer o fitxers" s'indica, respectivament: secretaria@xxx.cat, ajuntament@xxx.cat i alcaldia@xxx.cat.

Convé fer un petit incís per aclarir que l'Ajuntament pateix una confusió quan utilitza els models de sol·licitud previstos per a l'exercici del dret d'accés regulat a l'article 15 LOPD, per accedir a la part de la informació continguda en el fitxer *Outlook* corresponent a les adreces de correu esmentades. El dret d'accés previst a l'article 15 LOPD es reconeix al titular de les dades personals, que en aquest cas seria la funcionària local referida, la qual pot exercir aquest dret davant el responsable del fitxer *Outlook*, és a dir, l'alcalde d'aquest Ajuntament, i accedir a la informació corresponent a les adreces secretaria@xxx.cat, ajuntament@xxx.cat i alcaldia@xxx.cat. Altra cosa és el dret que deté l'alcalde (com a representant legal de l'Ajuntament), o bé la persona que aquest hagi autoritzat, d'accedir a la informació que sigui necessària per tal de complir amb les seves funcions, entre d'altres, vetllar per la seguretat de les dades recollides en l'exercici de les seves funcions, qüestió aquesta que analitzem en l'epígraf següent.

D'entre la documentació aportada consta un *report* dels *logs* o registres de les adreces de correu indicades, en concret, del següent: la data d'emissió de cada correu enviat des d'una d'aquestes adreces dins l'interval comprès entre l'1 ó 2 de setembre i el 23 d'octubre de 2009, el destinatari del correu i el codi d'identificació *Queue ID* corresponent a cada correu enviat.

En data 26 d'octubre de 2009 l'alcalde de l'Ajuntament incoa un expedient disciplinari a la funcionària local referida mitjançant el Decret d'alcaldia núm. 238/2009, l'apartat dels *Antecedents* del qual fa referència a un informe emès en data 23 d'octubre de 2009 per l'empresa xxx, com a encarregada de la implantació del sistema de seguretat dels fitxers automatitzats de dades de caràcter personal en aquest Ajuntament. En aquest mateix apartat s'assenyala el següent:

"D'aquest informe es desprèn que xxx ha pogut realitzar fets que són constitutius d'infracció normativa i conseqüentment de falta disciplinària.

1. *L'incompliment del deure de reserva professional pel que fa als assumptes que coneix per raó de les funcions que li són encomanades.*
2. *L'incompliment del deure de reserva professional pel que fa al tractament de dades protegides de caràcter personal."*

L'informe de 23 d'octubre de 2009 a què fa referència el Decret d'incoació de l'expedient disciplinari està emès per l'advocat i representant de l'empresa esmentada abans, i en aquest s'indica el següent:

“ Que el passat 16 d'octubre es va efectuar una sessió d'auditoria dels punts informàtics de l'Ajuntament de xxx, finalitzada la revisió es va considerar oportú demanar a l'Alcaldia que per motius de seguretat sol·licités un report dels correus electrònics a l'entitat que subministra el servei.

En el dia d'avui revistats els reports, es constata que el correu denominat secretaria@xxx.cat hi consta des del 9 de setembre i fins el 16 d'octubre del 2009, un total de 675 trameses, la major part de les quals a dues adreces (xxx@hotmail.com i xxx@xxx.com, que es poden considerar no oficials per a tràmits de l'Ajuntament de xxx, i també un gran nombre a (empty) que es podria considerar com correu ocult.

Davant d'aquests fets hi pot haver una presumpta fuga d'informació reservada i confidencial de l'Ajuntament de xxx, recomanant a l'Alcaldia que adopti mesures cautelars al respecte.”

Finalment, consten dos informes emesos també per l'empresa esmentada abans, un de data 11 de novembre de 2009, sobre el dret a la intimitat i el correu electrònic laboral, i un altre de data incerta, que porta per títol *Informe d'actuacions realitzades a l'Ajuntament de xxx*. Pel que fa a aquest segon informe, convé aclarir que en l'apartat *Seguiment* s'indica que “en data 11 de novembre de 2009 es comunicà la incidència a la directora de l'APDCAT, per tal que constés com a detectada”, i també que “es varen comunicar les mesures de caire legal adoptades”. Tot i aquesta afirmació, cal palesar que en el registre d'aquesta Agència no consta l'entrada d'aquest escrit ni de cap altre on s'hagi comunicat dita incidència, a banda òbviamment del coneixement que s'ha tingut a través d'aquesta consulta.

III

D'acord amb l'escrit de consulta, la instructora de l'expedient disciplinari considera que els fets relatats que són objecte de l'expedient disciplinari poden considerar-se una cessió o comunicació de dades de caràcter personal.

Sobre això, cal manifestar que dita afirmació pressuposa, en primer lloc, l'existència de *dades de caràcter personal*, és a dir, d'informació referent a persones físiques identificades o identificables (article 3.a de la LOPD); en segon lloc, pressuposa l'existència d'un o més *tractaments* de dades personals, entenent com a tals el conjunt d'operacions i els procediments tècnics de caràcter automatitzat o no que permetin recollir, gravar, conservar, elaborar, modificar, bloquejar i cancel·lar, així com les cessions de dades que derivin de comunicacions, consultes, interconnexions i transferències (article 3.c LOPD). El tractament al que es refereix la instructora, la cessió de dades, consisteix en qualsevol revelació de dades efectuada a una persona diferent de l'interessat (art. 3.i LOPD). Cal partir de la base que totes aquestes operacions, així com la gestió de la informació personal que se'n deriva, realitzades pels treballadors al servei d'un ajuntament en l'exercici de les tasques que els són assignades, han de regir-se per allò que disposa la normativa de protecció de dades.

Dels fets relatats en l'epígraf anterior es desprèn que la funcionària local referida té accés a tres fitxers que contenen dades de caràcter personal; que la mateixa funcionària considera que la informació que tracta en el desenvolupament de les seves tasques laborals requereix la màxima confidencialitat pel que fa a les dades personals tractades; que del 9 de setembre i fins el 16 d'octubre de 2009 s'han enviat 675 correus, amb un volum d'informació superior a 10 MB, des de

l'adreça de correu secretaria@xxx.cat, i que s'han enviat essencialment a dues adreces: xxx@hotmail.com i xxx@xxx.com, les quals es poden considerar adreces no oficials per a tràmits d'aquest Ajuntament, així com també a una adreça de correu que l'empresa esmentada abans indica com a *empty*, i que es podria qualificar com a correu ocult.

Tenint en compte aquesta informació es pot concloure el següent: si bé no es pot descartar que d'entre el volum d'informació enviada constin dades personals, sobretot tenint en compte les funcions que realitza dita funcionària i l'accés que té als tres fitxers esmentats, aquesta Agència no pot concloure a la vista de la informació de què disposa que s'hagi produït una cessió de dades personals, i això per diferents motius: en primer lloc, perquè aquesta Agència no té constància fefaent del fet que la funcionària local hagi revelat dades personals a una persona diferent de la persona o persones interessades, aquests són: el personal del propi Ajuntament, els proveïdors i deutors de l'Ajuntament i els contribuents dels tributs i taxes de l'Ajuntament, entre d'altres. Les declaracions on s'afirma que els destinataris dels correus enviats per la funcionària són adreces "no oficials", juntament amb el fet que la carpeta d'elements enviats des de l'*Outlook* de Secretaria té un volum molt elevat en comparació amb la carpeta d'entrada, tenint en compte el curt període de temps (de 9/09/09 a 1/10/09), concretament un volum superior a les 10 MB, entre d'altres, són fets objectius que, degudament acreditats, poden constituir indicis de la comissió d'una cessió de dades, però aquests indicis són certament insuficients en el marc d'un procediment sancionador o, com és el cas, disciplinari. Caldria tenir constància de la tramesa efectiva de dades personals. Però fins i tot si fos així, caldria acreditar l'autoria de la cessió, és a dir, caldria aportar elements de judici suficients que permetessin acreditar –tal vegada en aquest cas podria ser indiciàriament- que la funcionària imputada és la persona que ha efectuat la cessió. Però a més, cal tenir en compte que no totes les cessions de dades són il·legítimes i, per tant, sancionables, sinó només aquelles que contravenen les previsions de la LOPD, contingudes fonamentalment als articles 11 i 21 de la LPOD.

A banda de l'escrit pròpiament de consulta, en la Provisió de data 30 de novembre de 2009 la instructora manifesta la voluntat de sol·licitar informe a l'Agència "per tal que es pronunciï sobre si els fets descrits en l'expedient aportat constitueixen alguna infracció de les tipificades a la Llei orgànica de protecció de dades de caràcter personal, Llei 15/1999, de 13 de desembre".

La resposta en aquest cas ha de ser la mateixa. Si bé de la informació aportada a aquesta Agència es desprèn la detecció d'una incidència en el sistema de seguretat de la informació que pot posar en perill la seguretat de les dades personals, el cert és que no es constata cap tractament de dades personals, com podria ser la recollida, gravació, tramesa, destrucció, etc, de dades personals, sinó que només es presumeix. Per això, no es pot concloure que s'hagi comès una infracció de les previstes a la LOPD.

El mateix podríem dir de la imputació que s'assenyala en l'acord d'incoació de l'expedient disciplinari, fet mitjançant un decret d'alcaldia i consistent en "l'incompliment del deure de reserva professional pel que fa al tractament de dades protegides de caràcter personal". No és possible concloure que s'ha vulnerat el deure de reserva professional o el deure de secret a què fa referència l'article 10 LOPD si no hi ha constància del tractament de dades personals, això és, de dades que identifiquen una persona o bé que permeten la seva identificació fent un esforç raonable.

Sobre l'altra imputació que es fa en l'acord d'incoació, consistent en "l'incompliment del deure de reserva professional pel que fa als assumptes que coneix per raó de les funcions que li són encomanades", cal fer avinent que aquesta Agència no és competent per emetre una valoració sobre qüestions jurídiques que ultrapassin la normativa sobre protecció de dades, per la qual cosa

no emetrem cap observació. Per tant, les conclusions fetes fins ara s'emeten sens perjudici que els fets puguin constituir una o més infraccions d'altra normativa.

Dit això, es considera rellevant posar de manifest que són els responsables dels fitxers i els encarregats del tractament les persones que estan subjectes al règim sancionador que estableix la LOPD (article 43 LOPD). Igualment, els responsables dels fitxers o tractaments són les persones obligades a garantir la seguretat de les dades de caràcter personal evitant, entre d'altres, el tractament no autoritzat (art. 9 LOPD). Conseqüentment, en cas de cessió il·legítima seria el responsable del fitxer, i no el funcionari autor del tractament il·legítim, qui incorreria en responsabilitat. Altra cosa és que posteriorment el responsable del fitxer convingui incoar un expedient disciplinari al funcionari presumptament autor del tractament il·legítim per tal de depurar responsabilitats administratives, tal com preveu l'article 46 de la LOPD.

IV

Si bé els termes en els que s'ha plantejat la consulta no permeten emetre cap altra valoració, el contingut de la informació aportada ha posat de manifest que l'Ajuntament referit, directament o través de l'encarregat del tractament, ha exercit un control sobre el correu electrònic d'una empleada municipal, qüestió la qual té rellevància i actualitat des del punt de vista del dret a la protecció de les dades personals, i més en concret, pel que fa als límits i a les condicions d'exercici d'aquest control. Per això, a continuació s'analitzaran els criteris concrets que l'Ajuntament ha de tenir en compte des del punt de vista de la normativa de protecció de dades a l'hora d'exercir un control, en general, dels sistemes d'informació, i, en particular, del correu electrònic dels treballadors que directa o indirectament presten serveis públics per a dit Ajuntament.

Per tal que es consideri legítim el tractament de dades que pugui derivar del control exercit per l'Ajuntament dels sistemes d'informació, cal tenir en compte en primer lloc quina és la *finalitat* del control. En aquest sentit, és clar que l'Ajuntament ha de poder exercir un control quan aquest tingui per finalitat el manteniment de la infraestructura informàtica i telemàtica de què disposa (ordinadors, aplicacions, software i hardware, etc) per a que els seus treballadors compleixin amb les tasques que els són encomanades. Les tasques de manteniment i revisió, que poden comportar, entre d'altres actuacions, intervencions en els directoris de xarxa i en els ordinadors dels usuaris, són necessàries per a la detecció i eliminació dels elements que puguin causar problemes de funcionament dels sistemes d'informació. En definitiva, són necessàries per assegurar el correcte funcionament dels sistemes d'informació.

D'altra banda, la jurisprudència constitucional ha manifestat que el poder de direcció de l'empresari inclou facultats de control de l'activitat laboral. Pel que fa al control de l'ordinador, cal destacar la Sentència de 29 de setembre de 2007 dictada pel Tribunal Suprem en el recurs de cassació per a la unificació de doctrina núm. 966/2006, la doctrina de la qual fem extensible al control del correu electrònic. En el fonament de dret Tercer, l'Alt Tribunal assenyala, en relació amb un supòsit on és aplicable l'Estatut dels Treballadors (ET) que, a diferència de la taquilla o dels efectes personals del treballador, l'ordinador no forma part de l'esfera privada del treballador, sinó que és un instrument de producció, ja que a través del mateix el treballador executa la prestació del treball. L'empresari és el titular del dit ordinador, sigui com a propietari o per altre títol. Per això, no és aplicable l'article 18 ET –que estableix tota una sèrie de garanties per tal que el control sigui legítim-, sinó l'article 20.3 ET, la qual cosa significa que l'empresari pot controlar l'ús que fan els treballadors de l'ordinador per tal de verificar el compliment de la prestació del treball. En paraules de l'Alt Tribunal: *“el empresario ha de comprobar si su uso se ajusta a la finalidades que lo justifican, ya que en otro caso estaría retribuyendo como tiempo de trabajo el dedicado a actividades extralaborales”*.

En aquest sentit, es pot afirmar que l'Ajuntament, en la seva condició d'"empresari", també pot exercir un control quan aquest tingui per finalitat verificar el compliment per part dels treballadors de les seves obligacions laborals. Així, per exemple, si tenim en compte que l'article 54 de la Llei 7/2007, de 12 d'abril, de l'Estatut Bàsic de l'Empleat Públic (EBEP) estableix com a principi de conducta dels empleats públics, entre d'altres, el deure de no utilitzar els recursos i béns públics en benefici propi, l'Ajuntament podria realitzar actuacions de control de l'ordinador dels seus treballadors per tal de verificar el compliment d'aquest deure.

D'altra banda, la STS esmentada també considera legítim el control dels ordinadors de treball per part de l'empresari quan aquest tingui per finalitat coordinar i garantir la continuïtat de l'activitat laboral en els supòsits d'absència dels treballadors, i també (tot i que aquesta podria incloure's en alguna de les que ja hem esmentat), quan tingui per finalitat prevenir les responsabilitats que pot tenir l'empresa com a conseqüència d'alguna forma il·lícita d'ús de l'ordinador front a tercers.

Ara bé, cal tenir en compte que aquest dret que habilita l'empresari a realitzar un control de les eines de treball no és absolut sinó que està limitat per altres drets fonamentals, especialment, pel dret a la intimitat personal i familiar, el dret a l'honor i el dret a la pròpia imatge (article 18.1 de la Constitució), però també pel dret a la protecció de dades personals (article 18.4 de la Constitució) i pel dret al secret de les comunicacions (article 18.3 de la Constitució).

Per tal que dit control no suposi una intromissió il·legítima en el dret a la intimitat, en el dret a la protecció de dades personals, o en un altre dret dels esmentats abans, cal sotmetre dit control a l'anomenat *judici de proporcionalitat*, que el Tribunal Constitucional ha delimitat com l'examen de la mesura limitadora de drets respecte de l'objectiu perseguit (judici d'idoneïtat); si, a més, la mesura és necessària, en el sentit que no hi ha una altra mesura més moderada per a la consecució del propòsit buscat amb igual eficàcia (judici de necessitat); i, finalment, si la mesura és ponderada o equilibrada, per derivar-se'n més beneficis o avantatges per a l'interès general que perjudicis sobre altres béns o valors en conflicte (judici de proporcionalitat en sentit estricte). Pel que fa específicament al dret a la protecció de dades personals, cal tenir en compte el *principi de qualitat*, segons el qual les dades només es poden recollir i tractar quan siguin adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut les dades (article 4 de la LOPD).

Lligat amb el respecte als drets fonamentals esmentats, convé posar en relleu que en la STS esmentada l'Alt Tribunal supedita o condiona la legitimitat del control de l'ordinador dels treballadors al compliment per part de l'empresari del deure d'informar els seus treballadors sobre quines són les mesures de control dels sistemes d'informació. El Tribunal parteix del pressupòsit que existeix un hàbit generalitzat de tolerància a certs usos personals dels mitjans informàtics de l'empresa, i considera que això crea una expectativa de confidencialitat de l'ús que es faci d'aquests mitjans. Per això, segueix dient, si l'empresari vol exercir un control dels mitjans informàtics ha d'informar prèviament als treballadors sobre el contingut i abast de dit control (fonament jurídic Tercer).

En relació amb el cas concret, convé assenyalar que en l'informe emès per l'empresa esmentada que porta per títol *Informe actuacions realitzades a l'Ajuntament de xxx* s'assenyala a l'apartat Conclusions que l'Ajuntament ha advertit als usuaris dels fitxers des de l'any 2004 sobre quines són les seves obligacions i responsabilitats. Sobre aquesta afirmació, cal assenyalar que de la documentació que s'ha aportat a aquesta Agència no es pot constatar que l'Ajuntament hagi informat sobre aquests extrems als seus treballadors. En qualsevol cas, cal advertir que, d'entre la informació que es proporioni, cal explicar clarament quines seran les mesures de control de les eines de treball, entre elles el correu electrònic. I aquesta informació cal proporcionar-la abans

d'exercir el control. Fem aquesta observació per aclarir que el curs sobre les funcions i obligacions del personal de l'Ajuntament que segons consta en aquest mateix informe hauria realitzat l'empresa esmentada als treballadors de l'Ajuntament, és posterior als fets que han estat objecte de l'expedient disciplinari.

En relació amb el deure d'informació cal fer una segona observació. En l'informe emès en data 1 d'octubre de 2009 per l'operador de l'aplicació encarregat d'administrar i mantenir l'estructura dels fitxers automatitzats de dades de caràcter personal de l'Ajuntament, s'assenyalen les actuacions que va dur a terme el tècnic que va detectar la incidència, i és de veure que es refereix a les mesures de seguretat que apliquen als fitxers que tenen assignat un nivell *alt* de mesures de seguretat, d'entre les quals es troba la realització de "còpies de seguretat dels correus electrònics genèrics que es troben en funcionament a l'Ajuntament de xxx". Fem aquesta observació perquè els fitxers als quals té accés la funcionària local referida tenen assignat un nivell de mesures de seguretat bàsic (*Outlook*) i mitjà (*Comptabilitat i Tributs i Taxes*). L'aplicació de les mesures de seguretat de nivell alt a fitxers que tenen assignat un nivell bàsic o mitjà és possible, d'acord amb el que preveu l'article 81.7 del LROPD. Ara bé, en cas que sigui així, cal tenir en compte que l'Ajuntament haurà d'informar prèviament als seus treballadors de l'aplicació de les mesures de seguretat de nivell alt també als fitxers de nivell bàsic i mitjà, això és, que el control previst s'exercirà sobre tots els fitxers.

Per tot això es fan les següents,

Conclusions

Les dades de caràcter personal que tracta l'Ajuntament es troben sotmeses a la protecció específica de la normativa de protecció de dades, en concret, de la LOPD i el RLOPD, i per tant, aquest ha de respectar els principis i garanties que s'hi estableixen.

La informació de què disposa aquesta Agència sobre l'expedient disciplinari incoat a la funcionària local no permet concloure que s'hagi produït una cessió de dades i que aquesta sigui il·legítima, ni cap altre tractament de dades que comporti una infracció de la normativa de protecció de dades, sens perjudici de les conclusions a que pugui arribar la instructora de l'expedient disciplinari si disposa de més informació.

El control que exerceix l'Ajuntament sobre les eines de treball ha de respectar el marc normatiu aplicable i els límits establerts per la doctrina jurisprudencial, especialment els referits al respecte als drets fonamentals dels treballadors a la intimitat personal i familiar, l'honor i la pròpia imatge, la protecció de dades personals i el secret de les comunicacions.

L'Ajuntament pot exercir un control de les eines de treball, entre les quals es troba el correu electrònic, quan aquest control tingui per finalitat el manteniment de la infraestructura informàtica i telemàtica de què disposa l'Ajuntament, verificar el compliment per part dels treballadors de les seves obligacions laborals, o bé coordinar i garantir la continuïtat de l'activitat laboral en els supòsits d'absència dels treballadors. En tot cas, en aplicació del principi de qualitat (article 4 LOPD) cal determinar les actuacions de control en funció de la finalitat que es persegueixi en cada cas i escollir el sistema menys intrusiu per a les dades personals, en el benentès que no es poden tractar dades impertinents o excessives. També esdevé necessari informar clara i prèviament als treballadors sobre les seves obligacions, les mesures de seguretat implantades, així com l'abast del control de les eines de treball que s'exercirà per part de l'Ajuntament.