CNS 17/2009

Dictamen en relació amb la consulta plantejada per un representant sindical a un Ajuntament, respecte el contingut de la Instrucció "Sobre l'ús dels sistemes i tecnologies de la informació i comunicació per part del personal al servei de l'Ajuntament (...)"

Es presenta davant l'Agència Catalana de Protecció de Dades un escrit d'un ciutadà, en nom i representació d'un sindicat a l'Ajuntament, en relació amb la Instrucció del dit Ajuntament "Sobre l'ús dels sistemes i tecnologies de la informació i comunicació per part del personal al servei de l'Ajuntament (...)".

En l'escrit presentat es considera que la Instrucció posa en greu perill la confidencialitat de les dades personals dels ciutadans i dels propis treballadors i treballadores municipals. En concret, es demana el parer de l'Agència en relació amb les previsions de diversos apartats de la Instrucció, i d'altres que al criteri de l'Agència mereixin especial atenció.

Analitzada la consulta, que s'acompanya de fotocòpia de la Instrucció de l'Ajuntament sobre la qual es consulta, tenint en compte la normativa vigent aplicable i vist l'informe de l'Assessoria Jurídica, s'emet el següent dictamen.

I

(...)

II

La consulta del representant sindical es refereix a diversos apartats de la Instrucció de l'Ajuntament: "Sobre l'ús dels sistemes i tecnologies de la informació i comunicació per part del personal al servei de l'Ajuntament (...)" (en endavant, la Instrucció).

Per tal de situar la Instrucció en el seu context, cal dir que la Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local (en endavant, LRBRL), reconeix als municipis, en qualitat d'Administracions públiques de caràcter territorial, i dins l'esfera de les seves competències, la potestat d'autoorganització, entre d'altres (article 4). Segons disposa l'article 124.4.g) de la LRBRL als alcaldes els correspon la funció, entre d'altres, de dictar bans, decrets i instruccions. I mateix article 124 disposa, en el seu apartat 5 que:

> *"El Alcalde podrá delegar mediante decreto las competencias anteriores en la Junta de Gobierno Local, en sus miembros, en los demás concejales y, en su caso, en los coordinadores generales, directores generales u órganos similares, con excepción de las señaladas en los párrafos b), e), h) y j), así como la de convocar y presidir la Junta de Gobierno Local, decidir los empates con voto de calidad y la de dictar bandos. Las atribuciones previstas en los párrafos c) y k) sólo serán delegables en la Junta de Gobierno Local."*

En el cas que ens ocupa, la Instrucció la signa el Gerent de Recursos Humans i Organització. També cal tenir en compte el que disposa l'article 6 del Decret legislatiu 2/2003, de 28 d'abril, pel qual s'aprova el Text refós de la Llei municipal i de règim local de Catalunya. En concret, l'article 6 d'aquest Decret legislatiu disposa que:

" Els ens locals es regeixen pel que disposa la Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local, per aquesta Llei i totes les altres disposicions específiques i complementàries, i pel reglament orgànic i les ordenances pròpies de cada ens.

2 La legislació sobre règim local de la Generalitat de Catalunya garanteix als ens locals els àmbits normatius necessaris per a fer efectiu el principi d'autonomia organitzativa."

Així doncs, la Instrucció s'emmarca en la potestat d'autoorganització i, en concret, en el principi de jerarquia, adreçada als treballadors i treballadores al servei de l'Ajuntament. Així es desprèn de l'article 1 de la pròpia Instrucció, en el qual es delimita el seu objecte i àmbit d'aplicació:

"1. Aquesta instrucció té per objecte establir els criteris generals per a l'adequada utilització dels sistemes d'informació i comunicació, i en particular del correu electrònic i d'Internet, les quals es posen a disposició del personal al servei de l'Administració municipal per a l'exercici de les seves funcions.
2. Aquesta instrucció s'aplicarà al personal al servei de l'Ajuntament de ..., dels seus organismes autònoms i entitats públiques empresarials, així com, del personal de les societats mercantils que tinguin accés a aquests sistemes i mitjans d'informació."

Finalment, per tal d'emmarcar la finalitat d'aquest dictamen, cal dir que, tenint en compte les funcions de l'Agència, citades als efectes que ens ocupen en l'article 5.e) de la Llei 5/2002, i en l'article 15.1.g) del Decret 48/2003, de 20 de febrer, ja esmentats, l'Agència ha de donar resposta a les consultes formulades en el seu escrit pel representant sindical, des de la perspectiva de la normativa de protecció de dades de caràcter personal. No correspon, per tant, a l'Agència, informar sobre la pertinença, l'abast o el contingut en conjunt de la Instrucció de l'Ajuntament, sinó d'aquelles qüestions que han estat posades de manifest en la consulta que es formula, i aquelles altres que puguin ser rellevants des del punt de vista de la normativa de protecció de dades.

Per tant, a continuació es faran les consideracions que aquesta Agència considera pertinents, atesos els termes de la consulta formulada.

III

En la consulta es considera que algunes de les previsions de la Instrucció posen en greu perill la confidencialitat de les dades personals dels ciutadans i dels propis treballadors i treballadores municipals. Es pot deduir que en la consulta es manifesta la preocupació per què la protecció de les dades personals dels ciutadans i dels treballadors municipals no es dugui a terme correctament, vistos els termes de la Instrucció.

Per tal de centrar la qüestió objecte d'estudi en aquest dictamen, convé fer una aproximació general al dret a la protecció de dades de caràcter personal, configurat en l'article 18.4 de la Constitució espanyola, i al marc normatiu aplicable a aquest dret fonamental.

Com a punt de partida, tota aquella informació que tracta l'Ajuntament i que tingui la naturalesa d'informació de caràcter personal, estarà sotmesa a la protecció específica de la normativa de protecció de dades, en concret, de la Llei 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, LOPD), així com del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el reglament de desplegament de la LOPD (en endavant, RLOPD).

L'article 1 de la LOPD estableix que aquesta llei té per objecte garantir i protegir, pel que fa al tractament de les dades personals, les llibertats públiques i els drets fonamentals de les persones físiques, i especialment del seu honor i la seva intimitat personal i familiar.

Hem de definir les *dades personals* com qualsevol informació referent a persones físiques identificades o identificables (article 3.a) de la LOPD). És clar que el conjunt d'informació de caràcter personal que es pugui tractar en un Ajuntament, tant dels propis treballadors i treballadores municipals, com dels ciutadans, queden protegides per la normativa de protecció de dades personals, en concret, per la LOPD i el RLOPD, esmentades. La informació que pot arribar a tractar un Ajuntament en relació amb les seves competències i que no sigui informació relativa, directa o indirectament a persones físiques, no es trobarà protegida per la dita normativa, per bé que pot estar protegida per altra normativa sectorial aplicable (normativa tributària, de contractació, de propietat intel·lectual o industrial, per citar alguns exemples).

Suposa un *tractament* d'aquesta informació personal 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) de la LOPD). Totes aquestes operacions, i la gestió d'informació personal que se'n deriva, realitzades pels treballadors al servei de l'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.

La LOPD protegeix les persones físiques a través de la protecció de les seves dades personals, mitjançant l'aplicació d'una sèrie de principis i garanties que resulten exigibles en relació amb qualsevol tractament que es realitzi. Fent una aproximació general a aquests principis, sens perjudici de les concrecions que es faran més endavant en aquest dictamen, val a dir que qualsevol tractament de dades personals ha de donar compliment al 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).

Sense fer una relació exhaustiva, cal apuntar que hi ha d'altres principis i obligacions en la LOPD que s'han de complir en qualsevol tractament de dades personals, entre d'altres, el deure de donar informació als afectats sobre el tractament de les seves dades (article 5 LOPD); el deure de secret professional que s'imposa tant al responsable del fitxer com a qualsevol persona que intervingui en el tractament (article 10 de la LOPD); la obligació de crear, modificar o suprimir fitxers de titularitat pública, com serien els d'un Ajuntament, a través de disposició general publicada al diari oficial corresponent (per aplicació de l'article 20 de la LOPD); o bé les exigències que es deriven per a l'Ajuntament en cas que aquest prevegi l'accés a les dades personals per part d'un encarregat del tractament (article 12 de la LOPD). A més, la normativa de protecció de dades imposa l'aplicació de determinades mesures de seguretat als tractaments de dades, per part dels responsables dels fitxers o tractaments (article 9 de la LOPD). Aquests i altres principis i obligacions definits en la normativa de protecció de dades han de ser tinguts en compte, en tant que la Instrucció pot afectar dades de caràcter personal. Per tant, es pot afirmar que la interpretació que es faci dels articles de la Instrucció qüestionats en la consulta ha de ser coherent i respectuosa amb aquests principis i obligacions.

Per tant, tot i que no hi ha en la Instrucció referències generals i expresses a la legislació de protecció de dades (a banda de la menció a la "LOPD" feta en l'article 5.2, en relació amb les traces d'utilització derivades de la gestió d'aplicatius, apartat que es comentarà més endavant en aquest dictamen), cal interpretar el conjunt del contingut de la Instrucció, en allò que afecti al

tractament de dades de caràcter personal, en connexió amb els principis i obligacions que imposa la normativa de protecció de dades. Els principis i obligacions previstos en la LOPD són d'obligat compliment per a tota persona física o jurídica que tracti les dades personals, per tant, per al responsable del fitxer o tractament, entès com la persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que decideixi sobre la finalitat, el contingut i l'ús del tractament (article 3.d) de la LOPD), així com per a qualsevol persona que intervé en qualsevol fase del que hem denominat "tractament de dades".

Atesos els termes exposats en la consulta, caldrà tenir especialment en compte que la LOPD, com s'ha esmentat, imposa el deure de secret professional tant al responsable del fitxer o tractament com a qualsevol persona que intervingui en el tractament (article 10), de manera que el tractament de dades personals derivat de la Instrucció de l'Ajuntament ha d'assegurar el respecte per la confidencialitat de les dades personals, tant dels treballadors municipals com de qualsevol altra persona física.

IV

Com s'ha apuntat, la Instrucció disposa en el seu article 1 que el seu objecte és establir els criteris generals per a l'adequada utilització dels sistemes d'informació i comunicació, i en particular del correu electrònic i d'Internet, els quals es posen a disposició del personal al servei de l'Administració municipal per a l'exercici de les seves funcions. L'Ajuntament, d'aquesta manera, estableix en base a les competències que li atorga la normativa citada en l'apartat II d'aquest dictamen, pautes relatives a la utilització i la gestió dels sistemes d'informació per part dels seus treballadors i treballadores municipals, sistemes que han d'utilitzar habitualment per realitzar la seva feina.

Cal afegir que l'article 2 d'aquesta Instrucció especifica que aquesta "es complementarà amb les següents normes: "Norma respecte al Tractament de Dades de Caràcter Personal a l'Ajuntament (...)" (NPD) i "Norma Tècnica de Seguretat pels Usuaris dels Sistemes d'Informació de l'Ajuntament (...)" (NTS)." Atès que no es disposa d'aquests documents, el present dictamen es realitzarà tenint en compte, principalment, el contingut de la Instrucció que és objecte de consulta. En qualsevol cas, en tot allò que els documents citats afectin al tractament de dades personals, hauran d'interpretar-se conforme la normativa de protecció de dades personals.

Així doncs l'objecte d'aquesta Instrucció es refereix a la utilització de *sistemes d'informació* (en endavant, SI), que podríem considerar com el conjunt organitzat d'elements que s'interrelacionen i que poden ser elements físics, lògics i organitzatius que comporten el tractament d'informació de tot tipus, sigui de caràcter personal o no.

Amb caràcter general, podem dir que integren els SI d'una entitat o empresa, en el cas que ens ocupa, l'Ajuntament, el conjunt de persones o usuaris que integren la organització i utilitzen o tracten la informació, així com la pròpia informació, es tracti o no d'informació personal, i també el conjunt d'activitats o processos realitzats dins la organització en relació amb la informació tractada, els fluxos informatius que es generen, i també els recursos materials emprats en aquests processos. Als efectes de la normativa de protecció de dades, i segons disposa l'article 5.2.m) del RLOPD, constitueix un SI el conjunt de fitxers, tractaments, programes, suports i, si s'escau, equips utilitzats per al tractament de dades de caràcter personal. També haurem de tenir en compte que, segons el mateix article 5.2, apartat n) constitueix un sistema de tractament la manera en què s'organitza o utilitza un SI. És a dir, atenent al sistema de tractament, els SI poden ser automatitzats, no automatitzats o parcialment automatitzats.

V

Aquest comentari respecte el que podem considerar com SI, té rellevància als efectes de concretar la primera qüestió que la consulta sotmet al parer de l'Agència, que analitzem a continuació. Ens referim al contingut de l'article 4 de la Instrucció, relatiu a *l'Ús dels sistemes d'informació en general*, apartat 1, que té el redactat següent:

"Tots els recursos dels sistemes d'informació municipals, així com la informació continguda, són propietat de l'Ajuntament, pel que, no està permès el seu ús fora de les tasques assignades al seu lloc de treball."

En relació amb la frase: *"la informació continguda (als sistemes d'informació) són propietat de l'Ajuntament"* d'aquest apartat, en la consulta es considera que es passa per alt que la major part de la informació dels ciutadans, de les empreses i dels propis treballadors i treballadores municipals que resideix als sistemes d'informació municipals continua sent propietat dels seus titulars, que d'acord amb la llei conserven intactes tots els seus drets de protecció de les seves dades, amb totes les seves conseqüències.

En la consulta no es qüestiona que alguns dels elements que, com s'ha comentat, formen part d'un SI, puguin ser considerats com a propietat de l'Ajuntament o, caldria afegir, de tercers. La consulta qüestiona la propietat sobre un dels elements que formen part de tot SI, com és la informació, entesa en un sentit ampli. En concret, es qüestiona que es consideri a l'Ajuntament com a "propietari" de la informació continguda als SI, sense més distinció i amb caràcter general, vista la redacció de l'article 4 de la Instrucció.

La Instrucció es refereix a informació, en general, que pot ser de diversos tipus, com ja ha quedat dit. La informació que pot gestionar un Ajuntament pot referir-se a informació de la pròpia organització, o informació provinent de tercers, siguin persones físiques, empreses o institucions, altres administracions públiques, etc. La informació relativa a les diverses competències que exerceix un municipi, les quals es troben concretades en la normativa corresponent (articles 25 i següents de la LRBRL, i articles 8 i 9 –pel que fa a les potestats i competències dels ens locals-, i 66 –pel que fa a les competències municipals i locals- del Decret legislatiu 2/2003, entre d'altres), pot ser molt diversa.

Les competències municipals, i per tant la informació que pot tractar un Ajuntament, poden englobar matèries tan diverses com la seguretat en llocs públics, l'ordenació del trànsit o la protecció civil, la prestació de serveis socials i la participació en la gestió de l'atenció primària de salut, el patrimoni historicoartístic o les activitats culturals, l'exercici de competències en matèria de tributs, o la gestió del padró municipal d'habitants, entre d'altres, i simplement a tall d'exemple.

És clar que l'Ajuntament ha de tenir una capacitat de control i decisió sobre els SI que gestiona, i que posa a disposició dels seus treballadors per tal de complir amb les competències que la normativa atorga a l'Ajuntament. Més que en termes patrimonials, la referència feta en la Instrucció al terme "propietari", es pot entendre en el sentit que l'Ajuntament té aquesta capacitat de control i decisió en relació amb els SI i més en concret, en relació amb informació que, insistim, no és només informació personal. Des d'aquesta perspectiva general, l'Ajuntament és "propietari" de la informació.

Des de la perspectiva de la protecció de dades, certament la LOPD no es refereix als propietaris de la informació, sinó als responsables i als titulars de les dades personals. Pel que fa al responsable,

entès com la persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que decideixi sobre la finalitat, el contingut i l'ús del tractament (article 3.d) de la LOPD), la consideració de l'Ajuntament com a "propietari", resulta coherent amb la normativa de protecció de dades, si s'interpreta que l'Ajuntament és dipositari i responsable de la informació personal que tracta, en els termes de la LOPD.

No s'ha de confondre el concepte de "propietari" d'una informació amb el concepte d'"afectat o interessat", que segons l'article 3.e) de la LOPD és la persona física titular de les dades que siguin objecte del que hem definit com tractament de dades personals. A banda que, en base a les previsions de diversa normativa aplicable s'hagi de tractar la informació que gestiona un Ajuntament tenint en compte els drets o interessos que sobre la dita informació tinguin terceres persones físiques o jurídiques (per exemple, en matèria de contractació, o de gestió de serveis públics, o de propietat intel·lectual o industrial, etc), pel que fa a les dades de caràcter personal, cal tenir present que el dret fonamental a la protecció de dades (article 18.4 de la Constitució espanyola) es configura com un dret d'autodeterminació informativa que s'atorga als titulars de les dades, per tant, a les persones físiques (pel que fa a la concreció del contingut essencial d'aquest dret, ens remetem a la STC 292/2000).

Els titulars tenen un poder de control i disposició de la seva informació personal, amb la modulació que pugui establir-se en la normativa corresponent. Aquesta modulació porta, per exemple, a que la LOPD exceptuï en determinats supòsits la necessitat de comptar amb el consentiment del titular de les dades per a efectuar un tractament de les dades, o bé per a cedir-les a tercers (articles 6, 11 i 21 de la LOPD). D'aquesta manera la LOPD parteix de la base que, amb caràcter general, el tractament de les dades de caràcter personal requereix el consentiment inequívoc de l'afectat, llevat que la llei disposi una altra cosa. Aquesta previsió resulta plenament aplicable a qualsevol tractament de dades personals que es faci en el SI sobre el que es consulta.

En la consulta s'apunta que (els titulars) d'acord amb la llei conserven intactes tots els seus drets de protecció de les seves dades, amb totes les seves conseqüències. Certament, el dret a la protecció de dades personals, configurat com una autodeterminació informativa, atorga als titulars de les dades una sèrie de drets, anomenats drets ARCO o drets d*'habeas data* (drets d'accés, rectificació, cancel·lació i oposició) que el titular pot exercir en relació amb les seves dades, i envers qualsevol responsable d'un fitxer o tractament de les seves dades. Per tant, un titular de dades personals tractades per l'Ajuntament (un treballador municipal, un ciutadà, etc), sempre haurà d'estar en disposició d'exercir els seus drets ARCO i, si escau, de sol·licitar la tutela dels seus drets a les Agències de protecció de dades competents i de ser indemnitzats, tot això en els termes i condicions que estableix el Títol III de la LOPD.

Tenint en compte el contingut i configuració del dret a la protecció de dades de caràcter personal, la previsió de l'article 4 de la Instrucció, citada, s'hauria d'interpretar tenint en compte els conceptes d'afectat o interessat i de responsable, en els termes apuntats, així com els principis i obligacions que per a l'Ajuntament es deriven de la normativa de protecció de dades, i especialment l'exercici de drets ARCO per part dels interessats. En aquests termes, es pot considerar que la previsió de l'article 4 de la Instrucció resulta compatible amb la normativa de protecció de dades de caràcter personal.

VI

La consulta es refereix també al contingut de l'article 5 de la Instrucció, relatiu a *les Normes de manteniment i explotació dels sistemes d'informació,* apartat 1, que té el redactat següent:

"5.1. *Els tècnics informàtics responsables del manteniment i explotació dels sistemes d'informació vetllaran pel correcte ús de les eines de treball que l'Ajuntament posa a disposició del personal i, en aquest sentit, aquests estan facultats per efectuar les tasques de manteniment que siguin necessàries en els directoris de xarxa i en els ordinadors personals dels usuaris, per a la detecció i eliminació de tots aquells elements que, sense tenir relació amb les funcions a exercir en el lloc de treball, puguin causar problemes en el normal funcionament dels diferents elements que configuren les infraestructures informàtica i telemàtica del departament (jocs, protectors de pantalles, arxius d'àudio i vídeo, etc. no relacionats amb el lloc de treball, etc.).*

En concret, es qüestiona la frase: *Els tècnics informàtics (...) estan facultats per efectuar les tasques de manteniment que siguin necessàries en els directoris de xarxa i en els ordinadors personals dels usuaris, per a la detecció i eliminació de tots aquells elements (...).*

En la consulta es considera que s'està de fet autoritzant a aquest personal tècnic a inspeccionar el contingut de tots els repositoris d'informació que fan servir els usuaris de la Xarxa Municipal sense establir cap garantia, com ara comunicació prèvia a l'interessat o petició de cap autorització a cap responsable. S'afegeix en l'escrit formulat pel representant sindical que això es considera molt greu atès la naturalesa de la informació que es pot trobar, que passa a formar part d'una única i enorme base de dades documental, inclou dades de la més alta sensibilitat (filiació política, sindical, dades de caràcter fiscal i econòmic, dades relatives als Serveis Socials, etc). A més, s'afegeix, els tècnics informàtics al·ludits podrien ser molt bé operadors d'empreses externes contractats amb fórmules no sempre fiables.

Per tal de situar aquesta qüestió, cal partir de la base que l'Ajuntament, en tant que responsable dels fitxers o tractaments afectats per la Instrucció, té una sèrie d'obligacions tendents a assegurar que el tractament que es fa de les dades personals incloses en els fitxers sigui correcte i ajustat a la normativa de protecció de dades. En concret, l'article 9 de la LOPD estableix la obligació, per als responsables dels fitxers o tractaments, d'aplicar una sèrie de mesures de seguretat. L'apartat 1 d'aquest article disposa que:

> *"El responsable del fitxer i, si s'escau, l'encarregat del tractament han d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposats, tant si provenen de l'acció humana o del medi físic o natural."*

Les mesures de seguretat que són exigibles als fitxers i tractaments de dades de caràcter personal es classifiquen en tres nivells: bàsic, mitjà i alt, i en el Títol VIII del RLOPD es concreten les mesures tècniques i organitzatives que corresponen a cada nivell. En concret, l'article 81 precisa els nivells de seguretat que caldrà adoptar, en atenció a les categories de les dades personals tractades, de la finalitat del fitxer o tractament, i de que aquests fitxers i tractaments siguin manuals o automatitzats. El Títol VIII del RLOPD també concreta que caldrà consignar les corresponents mesures en el document de seguretat (article 88). Així doncs el responsable ha d'articular mesures que es refereixen, entre d'altres, al control d'accessos per part dels usuaris als recursos necessaris per exercir les seves funcions, a mesures que garanteixin la correcta identificació i autenticació dels usuaris, o a diverses mesures en relació amb la gestió de suports i documents. Algunes d'aquestes mesures impliquen, per exemple, que el responsable hagi d'implementar sistemes que permetin l'autenticació, és a dir, la comprovació de la identitat d'un usuari, a través d'una contrasenya o d'altres sistemes, si escau, o que hagi de comprovar quins són els accessos autoritzats a determinada informació, és a dir, conèixer i establir quines són les autoritzacions que cal concedir a cada usuari en relació amb la utilització de diversos recursos o informacions. També cal habilitar

un procediment de notificació i gestió de les incidències que afectin les dades de caràcter personal i s'ha d'establir un registre en què es faci constar el tipus d'incidència, el moment en què s'ha produït, o si s'escau, detectat, la persona que fa la notificació, a qui se li comunica, els efectes que se'n deriven i les mesures correctores aplicades.

És més, hem de tenir en compte allò que disposa l'article 89 del RLOPD, en relació amb les funcions i obligacions del personal, segons el qual:

> *"1.Les funcions i obligacions de cadascun dels usuaris o perfils d'usuaris amb accés a les dades de caràcter personal i als sistemes d'informació han d'estar clarament definides i documentades en el document de seguretat.*
>
> *També s'han de definir les funcions de control o autoritzacions delegades pel responsable del fitxer o tractament.*
>
> *2.El responsable del fitxer o tractament ha d'adoptar les mesures necessàries perquè el personal conegui d'una forma comprensible les normes de seguretat que afectin l'exercici de les seves funcions així com les conseqüències en què pugui incórrer en cas d'incompliment."*

També cal tenir present que el RLOPD exigeix que el responsable elabori un document de seguretat en el qual s'han de fer constar les mesures d'índole tècnica i organitzativa conformes amb la normativa de seguretat vigent que és de compliment obligat per al personal amb accés als SI (article 88). Específicament, l'apartat 3.c) d'aquest article exigeix que constin en el document de seguretat les:

> *"Funcions i obligacions del personal en relació amb el tractament de les dades de caràcter personal incloses en els fitxers."*

Partint d'aquesta base, és clar que l'Ajuntament ha d'explicar a totes aquelles persones que accediran i tractaran dades, principalment els treballadors municipals, quines són les mesures que han de tenir en compte, i quins són els procediments o protocols d'actuació. Amb caràcter general, es pot considerar que l'objectiu i contingut de la Instrucció s'emmarca en aquesta finalitat. En definitiva, és clar que qualsevol usuari, en el context del concepte de SI que hem utilitzat, ha d'estar assabentat de com ha gestionar els diferents elements que conformen el SI al qual té accés per realitzar la seva feina.

Més enllà de fer una relació completa de les mesures de seguretat previstes, o del contingut del document de seguretat, en relació amb la qual ens remetem a les previsions del RLOPD, es vol posar de manifest que el responsable, en el cas que ens ocupa, l'Ajuntament, té la obligació de vetllar pel compliment de les mesures de seguretat que imposa la normativa, les quals, en major o menor mesura, requereixen la implicació directa dels usuaris. Per tant, és evident que el personal que presta els seus serveis per compte d'un responsable, han de tenir constància de les mesures i de les implicacions que el seu compliment els genera. Es pot deduir que informar els usuaris i concretar els usos correctes dels SI per part d'aquests, en relació amb les seves funcions, constitueix l'objectiu de la Instrucció sobre la qual es demana el parer de l'Agència, objectiu que és respectuós, amb caràcter general, amb la normativa de protecció de dades, ja que dóna compliment a les obligacions de l'Ajuntament previstes en la normativa de protecció de dades en relació amb la gestió dels SI.

Per altra banda, en relació amb la consideració que es fa en la consulta de que els tècnics informàtics al·ludits podrien ser molt bé operadors d'empreses externes contractats amb fórmules no sempre confiables, des de la perspectiva de la protecció de dades és pertinent recordar les exigències que es deriven de la pròpia LOPD en preveure les condicions d'accés a les dades per compte de tercers. En concret, l'article 12 de la LOPD, en relació amb l'*encarregat del tractament,*

disposa que no es considera comunicació de dades l'accés d'un tercer a les dades quan l'accés sigui necessari per a la prestació d'un servei al responsable del tractament. En qualsevol cas, el tractament de dades de caràcter personal que hagi de realitzar un tercer per compte del responsable, en el cas que ens ocupa, per compte de l'Ajuntament, haurà d'estar regulada per un contracte, en el qual s'ha d'establir de manera expressa que l'encarregat només ha de tractar les dades d'acord amb les instruccions del responsable, que és qui decideix sobre la finalitat, contingut i usos del tractament. És especialment rellevant la previsió de l'article 12, citat, relativa a que l'encarregat del tractament no pot cedir o comunicar les dades a altres persones. Així mateix, l'encarregat del tractament, i les persones que treballen per a aquest encarregat, estan vinculades pel deure de secret respecte la informació que tracten (article 10 de la LOPD).

El document de seguretat, citat, és especialment important en el cas que l'Ajuntament encarregui a tercers el tractament de dades, ja que en aquest document s'han de concretar les característiques del tractament de dades personals que poden fer els encarregats del tractament, i hi haurà de constar la identificació dels fitxers o tractaments que han de tractar els encarregats, amb referència expressa al contracte o document que regula les condicions de l'encàrrec (article 88.5 LOPD). Per tant, la LOPD preveu una sèrie de controls i especificacions que ha de complir qualsevol encarregat del tractament que es contracti per part de l'Ajuntament.

Més enllà de les valoracions genèriques fetes en la consulta sobre la confiabilitat de determinades contractacions sobre les quals aquesta Agència no té elements per pronunciar-se, no es pot deduir de la Instrucció estudiada que l'Ajuntament no prevegi sotmetre's a les previsions de la LOPD i del RLOPD (articles 20 a 22) relatives a l'actuació de possibles encarregats del tractament.

Caldria afegir que tant si l'encarregat del tractament presta serveis en els locals del responsable, com si el servei es presta externament o es produeix un accés remot a les dades, en qualsevol cas aquest encarregat del tractament, i el personal al seu servei, ha de complir amb les mesures de seguretat que siguin pertinents en cada cas (article 82 del RLOPD).

Com hem apuntat, la normativa de protecció de dades imposa als responsables de fitxers i tractaments de dades una sèrie d'obligacions en relació amb l'aplicació de mesures de seguretat, les quals imposen la supervisió que aquestes mesures es compleixin, i la necessitat d'informar convenientment els usuaris, funció que compleix la Instrucció comentada.

És clar que, amb caràcter general, per poder donar compliment a les mesures de seguretat que imposa la normativa de protecció de dades segons el nivell exigible, el responsable ha de poder dur a terme, a través de persones designades per aquesta funció, com pot ser el personal tècnic informàtic en el cas que ens ocupa, diferents labors de comprovació del correcte ús de les eines de treball que l'Ajuntament posa a disposició del personal. Aquest treball s'ha de dur a terme sota el control, direcció i supervisió dels responsables designats a tal efecte pel responsable del fitxer o tractament.

És més, el Títol VIII del RLOPD, citat, estableix diverses previsions relatives a l'autorització que cal donar per a accedir a les dades personals i tractar-les. Amb caràcter general, l'article 84 del RLOPD disposa que les autoritzacions s'atribueixen al responsable, i que poden ser delegades en les persones designades a tal efecte. Tot i que la redacció de l'apartat 5.1 de la Instrucció, certament, no especifica quines persones estan designades per dirigir i supervisar les tasques que faran els tècnics informàtics, cal considerar plenament aplicables del previsions del Títol VIII del RLOPD en aquesta qüestió.

Com s'esmenta en l'apartat 5.1, qüestionat, la finalitat del manteniment és la detecció d'allò que podria causar problemes en el normal funcionament dels diferents elements que configuren les infraestructures informàtica i telemàtica del departament (jocs, protectors de pantalles, arxius d'àudio i vídeo, etc. no relacionats amb el lloc de treball, etc). Per tant, és clar que aquesta és la finalitat de les tasques de control, en els termes plantejats en la Instrucció.

La previsió de l'apartat 5.1 de la Instrucció respecte la intervenció dels tècnics informàtics, té una finalitat determinada, com és que es puguin efectuar les tasques de manteniment que siguin necessàries, en els directoris de xarxa i en els ordinadors personals dels usuaris, per a la detecció i eliminació dels elements que, sense tenir relació amb les funcions a exercir en el lloc de treball, puguin causar problemes de funcionament dels SI. La infraestructura informàtica i telemàtica de què disposa l'Ajuntament per a que els seus treballadors compleixin amb les tasques que els són encomanades, en definitiva, els ordinadors, aplicacions, software i hardware, etc, que formen part del que hem denominat SI, lògicament ha d'estar sotmesa a unes tasques de manteniment i revisió, per assegurar-ne el correcte funcionament.

Vist que l'aplicació i supervisió del correcte compliment de les mesures de seguretat pot comportar la realització, per part del responsable, de labors de supervisió dels diferents elements que conformen un SI, en el cas que aquestes tasques puguin comportar un accés a dades de caràcter personal, ja sigui de ciutadans o dels propis treballadors municipals, la pròpia LOPD exigeix que les dades de caràcter personal, en qualsevol cas, es tractin d'acord amb el principi de qualitat (article 4), i d'acord amb la finalitat concreta i legítima que justifica el tractament. Aquesta finalitat s'haurà de complir, per tal de resultar ajustada a la normativa de protecció de dades, conforme a les exigències del Títol VIII de la LOPD, al qual hem fet esment.

En especial, per aplicació del principi de qualitat, s'ha de tenir en compte l'exigència de proporcionalitat en el tractament de les dades, i el principi de minimització pel que fa a aquest tractament, entès com l'exigència de tractar només les dades personals que siguin estrictament necessàries per al compliment de la finalitat legítima. En aquest cas, això comporta que els tècnics informàtics només accedeixin i visualitzin la informació mínima necessària per realitzar les tasques de manteniment, i que no puguin tractar o utilitzar la informació per cap altra finalitat.

A tall d'exemple, citem la sentència del Tribunal Suprem, en unificació de doctrina, de 26 de setembre de 2007 (Fonament Jurídic cinquè), relativa al control de mitjans posats a disposició del treballador, en concret, l'ordinador personal.

> "Es cierto que la entrada inicial en el ordenador puede justificarse por la existencia de un virus, pero la actuación empresarial no se detiene en las tareas de detección y reparación, sino que, como dice con acierto la sentencia recurrida, en lugar de limitarse al control y eliminación del virus, «se siguió con el examen del ordenador» para entrar y apoderarse de un archivo cuyo examen o control no puede considerarse que fuera necesario para realizar la reparación interesada."

És clar que el principi de proporcionalitat, derivat del principi de qualitat de les dades, comporta no tractar més informació de la que sigui necessària per resoldre una incidència concreta que s'hagi produït en els SI, com ara la detecció d'un virus informàtic.

La consulta qüestiona part del contingut de l'apartat 5 de la Instrucció, apartat 2, que té el redactat següent:

"Així mateix, aquests responsables per garantir la continuïtat del servei i fer el seguiment de l'adequada utilització dels sistemes d'informació guardaran el rastre d'ús dels diferents aplicatius i sistemes. En concret, es mantindran els següents rastres:

- *Traces d'utilització derivades de la gestió de l'aplicatiu i les que imposi la LOPD.*
- *Registre de les accions fetes en els servidors de fitxers.*
- *Pàgines Internet visitades.*
- *Tràfic de la bústia de correu.*
- *Registre d'accés als sistemes d'aplicatius i recursos informàtics.*
- *Qualsevol altre registre que es requereixi per garantir el bon ús dels sistemes."*

Com hem vist, tant pel que fa a les dades i informació dels propis treballadors municipals com dels ciutadans en general, la consulta posa de manifest la preocupació per un ús indegut d'aquesta informació, que pot ser, a més, informació personal sensible als efectes de la LOPD. Cal analitzar, per tant, les implicacions que poden tenir per als drets dels usuaris, especialment els treballadors de l'Ajuntament, les mesures proposades en l'apartat 5.2 de la Instrucció.

Abans d'entrar en altres consideracions, cal deixar clar que la normativa de protecció de dades, efectivament estableix una protecció reforçada per les dades considerades sensibles (article 7). A banda d'altres consideracions fetes en l'article esmentat, al qual ens remetem, l'apartat 4 disposa que queden prohibits els fitxers creats amb la finalitat exclusiva d'emmagatzemar dades de caràcter personal que revelin la ideologia o l'afiliació sindical, entre d'altres. Si bé l'Ajuntament ha de tenir en compte les previsions de la LOPD respecte les dades sensibles, cal concloure, respecte d'aquesta qüestió, que de la lectura de l'apartat 5.1 de la Instrucció no es pot deduir que s'hagi de produir cap tractament d'informació personal que contravingui les previsions citades.

Pel que fa, en termes generals, a les dades dels ciutadans, ja ha quedat abastament exposat que el tractament que faci l'Ajuntament, en tant que responsable, així com qualsevol usuari, de les dades personals dels ciutadans, ha de cenyir-se a les exigències dels principis i garanties de la LOPD.

Pel que fa específicament a les dades dels treballadors municipals, i en connexió amb les exigències del principi de qualitat, citat, caldria recordar que els treballadors són titulars dels drets fonamentals que els corresponen en tant que ciutadans, i que aquests drets, com ha reiterat el Tribunal Constitucional, no deixen de tenir plena vigència en àmbit laboral, per bé que el seu exercici pot resultar modulat (SSTC 88/1985; 126/2003, entre d'altres). En aquest sentit, és clar que la vinculació contractual entre treballador i empresa no implica la privació del treballador dels drets que la Constitució li reconeix com a ciutadà, entre els quals, als efectes rellevants per aquest dictamen, el dret fonamental a la intimitat personal i familiar, el dret a l'honor i el dret a la pròpia imatge (article 18.1 de la Constitució) i òbviament, el dret a la protecció de dades personals (article 18.4 de la Constitució). També caldrà tenir en compte el que es desprèn del dret fonamental al secret de les comunicacions, configurat en l'article 18.3 de la Constitució. Aquests drets, a banda del que ja s'ha dit en matèria de protecció de dades, reben protecció específica en àmbit civil (Llei orgànica 1/1982, de 5 de maig, de protecció civil dels drets a l'honor, la intimitat personal i familiar i la pròpia imatge), i penal (a través de la figura del delicte de descobriment i revelació de secrets, regulada als articles 197 i següents del Codi Penal).

Citem a continuació les previsions en la normativa sectorial aplicable a l'àmbit que ens ocupa, per tal de delimitar els controls o intromissions legítimes que una organització o empresa, en aquest cas, un Ajuntament, pot realitzar respecte els drets dels seus treballadors.

En l'àmbit municipal, segons l'article 21.1 de la LRBRL, citada, l'Alcalde ostenta l'atribució de dirigir el govern i l'administració municipal, així com, entre d'altres, la de *"desempeñar la jefatura superior de todo el personal, y acordar su nombramiento y sanciones, incluida la separación del servicio de los funcionarios de la Corporación y el despido del personal laboral".* En el mateix sentit, l'article 53.1.b) del Decret legislatiu 2/2003, citat, estableix que l'alcalde dirigeix el govern i l'administració municipals. Per tant, l'alcalde dirigeix l'administració municipal, incloent el personal que presta serveis en l'Ajuntament. Finalment, l'article 92.1 de la LRBRL afegeix, pel que fa als funcionaris al servei de l'Administració local, que es regeixen, en allò que no prevegi la Llei de bases, per la legislació de l'estat i de les Comunitats autònomes en els termes de l'article 149.1.18ª de la Constitució.

Segons disposa l'article 2.1 de la Llei 7/2007, de 12 d'abril, de l'Estatut Bàsic de l'Empleat Públic (EBEP), aquest s'aplica al personal funcionari i en allò que procedeixi al personal laboral al servei de les administracions públiques, entre d'altres, les Administracions de les entitats locals. En l'article 14 de l'EBEP es reconeixen els drets individuals dels empleats públics, entre d'altres, el respecte de la seva intimitat, pròpia imatge i dignitat en el treball, i demés drets reconeguts per l'ordenament jurídic. L'article 52 de l'EBEP concreta els deures dels empleats públics i els principis que inspiren el codi de conducta que aquests han de complir. A més, aquest article especifica que els principis i regles establerts en el Capítol VI de l'EBEP informen la interpretació i aplicació del règim disciplinari dels empleats públics, concretat en els articles 93 i següents. L'exercici de la potestat disciplinària correspon a cada Administració pública respecte el personal al seu servei, en el cas que ens ocupa, correspon a l'Ajuntament (article 94 de l'EBEP). L'article 54 de l'EBEP concreta els principis de conducta dels empleats públics, entre d'altres, desenvolupar les tasques corresponents al seu lloc de treball de forma diligent i obeir les instruccions i ordres professionals dels seus superiors, així com administrar els recursos i béns públics amb austeritat, i no utilitzar-los en profit propi o de persones properes. Tenen, també, el deure de vetllar per la conservació d'aquests recursos i béns.

Respecte el personal laboral, l'article 92 de l'EBEP disposa que el personal laboral es regirà per l'Estatut dels Treballadors (ET), aprovat per Reial decret legislatiu 1/1995, de 24 de març i pels convenis col·lectius que siguin d'aplicació. L'ET preveu els drets bàsics dels treballadors, entre els quals, als efectes que ens ocupen, es cita el respecte per la seva intimitat i la consideració deguda a la seva dignitat (article 4). Com ha posat de manifest la jurisprudència constitucional, el poder de direcció de l'empresari, inclou facultats de control de l'activitat laboral. Així, l'article 20.3 ET atribueix a l'empresari, entre d'altres, la facultat d'adoptar les mesures que estimi més oportunes de vigilància i control per a verificar el compliment pel treballador de les seves obligacions laborals amb el degut respecte per la dignitat del treballador.

Tot i que els drets fonamentals dels treballadors no poden impedir amb caràcter general l'exercici d'aquestes facultats per part de l'empresari, sí és cert que modulen la seva possibilitat de control, en el sentit que s'han de respectar sempre aquests drets. El control del grau de compliment laboral no pot, en qualsevol cas, suposar una intromissió il·legítima en els drets a la intimitat o a la protecció de dades dels treballadors, entre d'altres.

En definitiva, la limitació de drets fonamentals dels treballadors en el marc de les relacions laborals, ha de complir amb l'anomenat judici de proporcionalitat, que el Tribunal Constitucional ha delimitat com l'examen respecte l'objectiu proposat amb la mesura limitadora de drets (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). Simplement a tall d'exemple, i en relació amb la limitació de drets fonamentals esmentats en l'àmbit laboral, citem les SSTC 186/2000 i 98/2000. En qualsevol cas, tota limitació de l'exercici de drets fonamentals dels treballadors, per part de l'empresari, ha de ser una mesura prevista en una norma amb rang de llei, proporcionada i necessària en una societat democràtica, com es desprèn de la jurisprudència constitucional.

En relació amb la utilització de dades personals dels treballadors, el Tribunal Constitucional ha manifestat que el dret de control del flux informatiu tracta d'evitar que la informació de les dades personals propiciï comportaments discriminatoris. En la STC 94/1998, s'ha reconegut que un tractament inadequat de dades personals dels treballadors pot posar en risc el legítim exercici de drets fonamentals dels treballadors, per exemple, la llibertat sindical, en connexió amb el dret a la protecció de dades personals. La STC citada examina un supòsit en que s'havia utilitzat una dada especialment sensible, com és l'afiliació sindical d'un treballador, que es facilita única i exclusivament a efectes de descomptar de la retribució la corresponent quota sindical. No obstant això, la dada va ser utilitzada per a retenir la part proporcional del salari relativa a un període de vaga. Com destaca el Tribunal:

"...se utilizó un dato sensible, que había sido proporcionado con una determinada finalidad, para otra radicalmente distinta con menoscabo del legítimo ejercicio del derecho de libertad sindical."

Més en concret, val a dir que la jurisprudència ha examinat diversos casos en què es plantegen els límits del registre, per part de l'empresari, de les eines de treball que posa a disposició del treballador, com ara els telèfons, els ordinadors, etc, També s'ha fet especial atenció a les possibilitats de control de la utilització que fan els treballadors de les noves tecnologies, com ara les connexions a Internet, i a l'ús correcte que ha de fer el treballador d'aquestes eines, en especial d'Internet i el correu electrònic (entre d'altres, la STSJ de Catalunya, d'11 de març de 2004, o la STSJ de la Comunitat de Madrid, de 16 de gener de 2008).

En alguns casos s'ha admès, per exemple, com a respectuós amb el dret a la intimitat dels treballadors, la col·locació en xarxa de programes que permeten verificar, sense entrar en l'ordinador de l'usuari, quin ús en fa aquest, en concret, per controlar la pràctica de jocs durant la jornada laboral, considerant que es tracta d'una mesura idònia i proporcionada (STSJ de Catalunya, de 29 de gener de 2001).

Als efectes que ens ocupen, recordem la STS de 26 de setembre de 2007, citada, relativa al control de mitjans posats a disposició del treballador, en concret, l'ordinador personal, i l'ús que aquest en pot fer. Com es desprèn d'aquesta sentència, el control esmentat s'emmarca en allò previst en l'article 20.3 de l'Estatut dels Treballadors, segons el qual:

> *"El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana (...)."*

Es constata en aquesta sentència que en l'ús del treballador dels mitjans informàtics facilitats per l'empresa poden produir-se conflictes que afecten la intimitat dels treballadors tant en el correu electrònic, en el qual la implicació s'estén també al dret fonamental al secret de les comunicacions, com en la denominada "navegació" per Internet, i en l'accés a determinats arxius personals de

l'ordinador. El conflicte existeix, com afegeix la sentència, perquè existeix una utilització personalitzada i no merament laboral o professional d'aquests mitjans (Fonament Jurídic segon).

Dit això, el TS afegeix que el control dels ordinadors es justifica per la necessitat de coordinar i garantir la continuïtat de l'activitat laboral en els supòsits d'absències dels treballadors, per la protecció del sistema informàtic de l'empresa, que pot ser afectat negativament per determinats usos, i per la prevenció de les responsabilitats que per a l'empresa puguin derivar de formes il·lícites d'ús front a tercers (Fonament Jurídic tercer):

> "(...) es necesario recordar (...) la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio. Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios con aplicación de prohibiciones absolutas o parciales e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado «una expectativa razonable de intimidad» en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (TEDH 1997, 37) (caso Halford) y 3 de abril de 2007 (TEDH 2007, 23) (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo par la protección de los derechos humanos."

Per tant, pel que fa a l'article 5.2 de la Instrucció, s'habilita un rastreig d'informació per garantir la continuïtat del servei i fer el seguiment de l'adequada utilització dels SI per part dels treballadors. Partint de la base, que ja s'ha esmentat, que en la mesura que aquestes finalitats poden afectar a dades sotmeses a la normativa de protecció de dades personals, cal comptar amb el consentiment de l'afectat, o bé amb una norma amb rang de llei que habiliti el tractament sense disposar d'aquest consentiment. Per tant, cal atendre al marc normatiu aplicable, pel que fa a la capacitat de control de l'Ajuntament i a la manera d'articular aquest control, i també cal tenir present la jurisprudència rellevant en aquesta matèria, per tal d'assegurar el respecte pels drets fonamentals dels treballadors.

Especialment, com es desprèn de la jurisprudència rellevant en aquesta matèria, cal posar de manifest la importància del compliment del deure d'informació per part de l'empresa, en el cas que ens ocupa, l'Ajuntament, respecte els seus treballadors, en relació amb el compliment de les finalitats de la Instrucció, i en relació amb mesures concretes de control dels SI. Cal que es doni informació suficient i clara als treballadors, amb caràcter general, sobre les mesures de control que s'apliquen, sobre la informació que es tracta per aplicació d'aquests controls i sobre les repercussions que pot tenir un ús inadequat dels SI. Si l'Ajuntament, en el cas que ens ocupa, estableix unes regles d'ús dels SI a través de la Instrucció i n'informa adequadament els treballadors, aquests poden tenir un coneixement adequat sobre la utilització correcta dels SI. Aquesta informació, doncs, és necessària per a l'exercici legítim de control per part de l'Ajuntament respecte les eines esmentades, i per a efectuar determinades actuacions de control, si escau, en relació amb l'ús d'aquestes eines, en aplicació al marc normatiu al que hem fet referència.

VIII

Finalment, cal fer esment de la previsió, en l'article 5.2 de la Instrucció del "manteniment" del rastre d'ús dels diferents aplicatius i sistemes. En la consulta es considera que quan es parla de crear i explotar registres de les pàgines d'Internet visitades o del tràfic de la bústia de correu, o d'altres que es considerin necessaris, "s'està de fet creant bases de dades de caràcter personal sense cap mena de control ni declaració".

La Instrucció informa de que es mantindran rastres de pàgines web visitades i de tràfic de bústia de correu, entre d'altres. Respecte de les pàgines web visitades, la informació recollida a què es refereix l'article 5.2 pot ser, per exemple, les adreces de les pàgines web visitades, l'hora i el temps de connexió a la pàgina visitada, la IP i dades identificatives de la persona física o usuari que visita aquestes pàgines, entre d'altres. Pel que fa al tràfic de la bústia de correu, la informació recollida podria ser l'adreça de correu i la IP d'origen –en relació amb l'ordinador des del qual s'envia el missatge- així com l'adreça de correu i la IP del destinatari del correu, així com l'assumpte o encapçalament del missatge, i la data i l'hora dels missatges, principalment. En un i altre cas, en funció de la configuració que s'estableixi dels SI, la informació que es pot arribar a tractar pot ser més o menys àmplia.

En concret, en relació amb la IP, aquesta Agència ha tractat la seva possible configuració com a dada personal en el Dictamen 1/2008, en els següents termes (Fonament Jurídic II):

"En concret, s'ha de fer una especial referència a la dada relativa a l'adreça IP. Aquesta dada en principi s'associa a un ordinador, el qual pot tenir un nombre divers o indeterminat d'usuaris, però pot arribar a associar-se a una o més persones físiques concretes. A partir de la normativa aplicable a la protecció de dades, citada, cal fer esment del Dictamen 4/2007, de 20 de juny, sobre el concepte de dades personals, elaborat pel Grup de Treball de l'Article 29 de la Directiva 95/46/CE. En aquest dictamen el Grup considera les adreces IP com dades sobre una persona identificable. En concret, i com ja s'havia considerat en l'anterior Document de treball del Grup, "Privacitat a Internet: -enfocament comunitari integrat de la protecció de dades en línea-", de 21 de novembre de 2000, els proveïdors d'accés a Internet i els administradors de xarxes locals poden identificar per mitjans raonables als usuaris d'Internet als quals han assignat adreces IP, ja que enregistren sistemàticament la data, hora, durada i adreça IP dinàmica assignada (...). "

Per tant, tot i que a l'adreça IP no se li pot atribuir, aïlladament considerada, la consideració de dada personal, sí haurà de tenir aquesta consideració en tots aquells casos en què pot fer identificable una persona física determinada. Vist el context de la Instrucció, i el seu abast en relació amb els treballadors d'una organització concreta com és un Ajuntament, que seran identificables, es podria considerar la IP com a dada de caràcter personal.

En qualsevol cas, a banda de les consideracions fetes en relació amb la IP, tenint en compte que qualsevol informació sobre persones físiques identificades o identificables ha de ser qualificada com dada de caràcter personal i, per tant, sotmesa a la LOPD, és clar que el manteniment de la informació derivada d'aquests rastres, previst en l'article 5.2 de la Instrucció, afecta a dades considerades de caràcter personal. Si considerem que els diferents supòsits de rastreig explicitats en l'article 5.2 de la Instrucció poden contenir en conjunt dades de caràcter personal, i que fins i tot es pot donar un perfil sobre comportament de persones concretes, és clar que s'està generant un tractament de dades personals, als efectes de l'article 3.c) de la LOPD.

També hem de tenir en compte que, si bé és cert que el funcionament dels SI comporta que es guardin de forma automàtica certs registres, no és aquest el supòsit a què es refereix la Instrucció, sinó que de la redacció de l'article 5.2 es dedueix una decisió de l'Ajuntament de conservar la informació referida, per donar compliment a les finalitats de control de la Instrucció, decisió que comporta un tractament de dades personals, als efectes de la LOPD.

Vist que l'article 5.2 de la Instrucció estableix clarament que "es mantindran" determinats rastres que, com ha quedat dit, comporten el tractament de dades personals per al compliment de les finalitats de la Instrucció, serà necessària la creació del corresponent fitxer o fitxers de dades personals per part de l'Ajuntament, en tant que responsable del tractament. La previsió de l'article 5.2 comporta la conservació i el tractament de dades personals, i en conseqüència aquest tractament ha d'estar ajustat al que disposa la LOPD (article 20) i el RLOPD (article 54), pel que fa a la creació de fitxers, i a la Llei 5/2002, de l'Agència, pel que fa a la inscripció corresponent al Registre de Protecció de Dades de Catalunya.

Es fa avinent que l'article 5.2 és inconcret en la seva última referència, relativa a "qualsevol altre registre que es requereixi per garantir el bon ús dels sistemes". En aquest sentit, no es dóna informació concreta als usuaris sobre quin tipus de registre o informació es pot rastrejar. Com s'ha esmentat abastament, la informació que es dóna als usuaris per part dels responsables, en aquest cas, de l'Ajuntament, en relació amb l'ús correcte dels SI i les conseqüències d'aquest ús, té una importància especialment rellevant, i per tant seria recomanable una major concreció en aquest punt.

Respecte els usuaris que poden ser afectats pel rastreig establert en l'article 5.2 de la Instrucció, no es dóna informació concreta, per la qual cosa els usuaris podrien ser tots els treballadors de l'Ajuntament, o bé es podria configurar un rastreig només en relació amb determinats usuaris, en atenció a diversos criteris.

Finalment, apuntar que no es disposa d'informació en relació amb el temps de conservació o manteniment dels rastres d'ús d'aplicatius i sistemes. En aquest sentit, en relació amb les dades personals tractades, caldrà tenir en compte que la LOPD exigeix la seva cancel·lació quan el tractament de dades ha deixat de ser necessari per a la finalitat que el justifica (article 4.5 de la LOPD). A més, la cancel·lació dóna lloc al bloqueig, i les dades només s'han de conservar en els casos previstos en l'article 16 de la LOPD. Als efectes de concretar el temps de conservació adequat, caldria tenir en compte que, amb caràcter general, no sembla justificat mantenir o guardar rastres respecte l'ús de SI, en concret, les dades personals que se'n derivin, de forma indefinida, a menys que la finalitat legítima ho justifiqui. Per tant l'Ajuntament haurà de tenir en compte les previsions de la LOPD pel que fa al temps de conservació d'informació associada directa o directament a persones físiques usuàries dels seus SI, en relació amb les previsions de l'article 5.2 de la Instrucció.

Per tot això es fan les següents,

Conclusions

Les dades de caràcter personal que tracta l'Ajuntament en aplicació de la Instrucció objecte de consulta es troben sotmeses a la protecció específica de la normativa de protecció de dades, en concret, de la LOPD, i per tant les previsions de la Instrucció han de respectar aquesta normativa i interpretar-se d'acord amb els principis i garanties que s'hi estableixen.

L'article 4 de la Instrucció *"...la informació continguda (als sistemes d'informació municipals) són propietat de l'Ajuntament..."* s'ha d'interpretar tenint en compte el concepte d'afectat o interessat (article 3.e) de la LOPD), i els principis i obligacions que per a l'Ajuntament es deriven de la normativa de protecció de dades, per tal de respectar l'autodeterminació informativa de l'interessat, específicament la necessitat de requerir el consentiment del titular, si escau, i la possibilitat d'exercir els drets ARCO.

En aplicació del principi de qualitat (article 4 de la LOPD) les labors de manteniment i comprovació del correcte ús de les eines de treball que l'Ajuntament posa a disposició del personal, realitzades pel personal tècnic informàtic, han de servir única i exclusivament per garantir el normal funcionament dels sistemes, per a la detecció d'incidències i per a solucionar-les convenientment.

El legítim exercici de control de l'empresa sobre les eines esmentades, amb les finalitats establertes en l'article 5.2 de la Instrucció, s'ha de mantenir en els termes establerts en el marc normatiu aplicable i en la jurisprudència, per tal d'assegurar el respecte pels drets fonamentals dels treballadors.

L'article 5.2 de la Instrucció estableix el manteniment de determinats rastres que comporten el tractament de dades personals per al compliment de les finalitats de control previstes a la Instrucció, i per tant serà necessària la creació del corresponent fitxer o fitxers de dades personals per part de l'Ajuntament, en tant que responsable del tractament, als efectes del que disposa la LOPD (article 20) i el RLOPD (article 54), i la inscripció corresponent al Registre de Protecció de Dades de Catalunya.