Dictamen en relació amb la consulta plantejada per un sindicat sobre l'adequació del Manual de bones pràctiques de l'usuari dels recursos informàtics d'un ajuntament a la normativa de protecció de dades

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit emès pel secretari general d'un sindicat sobre l'adequació del Manual de bones pràctiques de l'usuari dels recursos informàtics d'un ajuntament a la normativa de protecció de dades.

A l'escrit de consulta s'adjunta còpia de l'esmentat Manual de bones pràctiques de l'usuari dels recursos informàtics de l'Ajuntament.

Analitzada la petició i la documentació que l'acompanya, i vist l'informe de l'Assessoria Jurídica, es dictamina el següent:

I

(...)

II

El secretari general del sindicat manifesta, en el seu escrit de consulta, que l'Ajuntament ha lliurat als seus treballadors el Manual de bones pràctiques de l'usuari dels recursos informàtics (en endavant, el Manual de bones pràctiques), en què s'estableixen les regles segons les quals ha de comportar-se el personal de la Corporació en relació amb l'ús de les Tecnologies de la Informació i la Comunicació (TIC).

Tot seguit, afegeix que diverses previsions d'aquest Manual de bones pràctiques no s'ajustarien, segons el seu parer, a la normativa en matèria de protecció de dades de caràcter personal, motiu pel qual sol·licita el corresponent dictamen d'aquesta Autoritat.

Cal apuntar, en aquest punt, que les previsions assenyalades pel sindicat fan referència, principalment, als aspectes següents:

a) El concepte de responsable del tractament de dades de caràcter personal (lletra e) de l'escrit).
b) El control que l'Ajuntament pot exercir sobre l'ús de les TIC posades a disposició dels treballadors públics (lletres b), h) i n) de l'escrit).
c) Les mesures de seguretat a implementar en el tractament de les dades personals (lletres a), c), d), g), i), l) i m) de l'escrit).
d) Altres qüestions de caràcter més general (lletres f), j) i k) de l'escrit).

A continuació, s'analitzen les qüestions posades de manifest pel sindicat en el seu escrit de consulta -si bé s'ha optat per agrupar-les per àmbits- que resultin rellevants des del punt de vista de la protecció de les dades personals, que és la perspectiva des de la qual s'emet aquest dictamen. No correspon, per tant, a aquesta Autoritat, informar sobre la pertinença, l'abast o el contingut d'altres aspectes del Manual de bones pràctiques de l'Ajuntament.

III

El sindicat assenyala que l'apartat 5.5 del Manual de bones pràctiques, en què l'Ajuntament disposa que tota la informació que es faci servir en l'àmbit de treball de l'empleat és de propietat exclusiva de la Corporació i, per tant, no se'n pot fer un ús privat, podria contradir la normativa de protecció de dades.

S'entén que, atès el redactat emprat en aquest apartat, el que es qüestiona és que l'Ajuntament es consideri el "propietari" de la informació continguda al sistema d'informació, sense més distinció i amb caràcter general.

Cal fer avinent que la informació que pot gestionar l'Ajuntament en exercici de les seves competències –concretades en la legislació de règim local (Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local, i 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)- pot ser molt diversa i pot incloure, o no, dades de caràcter personal, enteses com *"qualsevol informació referent a persones físiques identificades o identificables"* (article 3.a) Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD)).

És a dir, les competències que aquest exerceix –i, per tant, la informació que pot tractar- poden englobar matèries tan diverses com, entre d'altres, 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.

En aquest sentit, és clar que l'Ajuntament ha de tenir una capacitat de control i decisió sobre els sistemes d'informació que gestiona i que posa a disposició dels seus treballadors per tal de complir amb les competències que la legislació de règim local li atribueix.

La referència feta en aquest apartat 5.5 del Manual de bones pràctiques al terme "propietari" es pot entendre, per tant, en el sentit que l'Ajuntament té aquesta capacitat de control i decisió en relació amb els sistemes d'informació i, més en concret, en relació amb la informació que, convé apuntar, podria no ser només informació de caràcter personal. Des d'aquesta perspectiva general, per tant, es podria considera que l'Ajuntament és "propietari" de la informació dels sistemes d'informació.

Dit això, cal fer avinent que, tal i com apunta el sindicat, és cert que, des de la perspectiva de la protecció de dades, la LOPD no es refereix als "propietaris" de la informació, sinó als responsables i als titulars de les dades de caràcter personal. Així, d'acord amb el seu article 3, es considera que és responsable del fitxer o tractament *"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"* (apartat d) i afectat o interessat *"la persona física titular de les dades que siguin objecte del tractament"* (lletra e).

Tenint en compte, doncs, aquests conceptes d'afectat i de responsable del fitxer o tractament de la LOPD, cal fer avinent que, en la mesura que la consideració de l'Ajuntament com a "propietari" de les dades personals s'interpreti en el sentit que aquest és dipositari i responsable del tractament de les dades personals necessàries per a l'exercici de les seves competències, siguin els ciutadans o els treballadors els seus titulars, es pot entendre que la previsió de l'apartat 5.5 del Manual de bones pràctiques resulta conforme amb la normativa de protecció de dades, tot i que resultaria més adequat, des del punt de vista de la protecció de dades, qualificar-lo com a "responsable".

IV

D'altra banda, el sindicat assenyala que les previsions dels apartats 2.3 i 7.3 del Manual de bones pràctiques, així com de l'annex del Manual, de data de 10 d'octubre de 2012, totes elles relacionades amb el control que l'Ajuntament pot exercir sobre l'ús que els treballadors fan de les TIC, podrien no adequar-se a la normativa de protecció de dades.

L'apartat 2.3 estableix, en relació amb l'ús de programari, que *"qualsevol programari no autoritzat que s'instal·li en un equip de la corporació pot ser esborrat des del Servei d'Informàtica de forma automàtica en qualsevol moment i sense cap advertència o comunicació prèvia".*

L'apartat 7.3 estableix, en relació amb l'ús del correu electrònic, que *"l'Ajuntament podrà controlar els missatges de correu electrònic quan hi hagi indicis que s'ha vulnerat la present política d'utilització del correu electrònic o per causa d'alguna obligació legal".*

Per la seva part, a l'annex s'estableix que *"(...) s'autoritza de forma informada i expressa a l'administrador del sistema a que revisi i inspeccioni els logs dels accessos dels usuaris de l'ajuntament a Internet com les direccions dels correus rebuts i enviats, sense que aquesta actuació de revisió i inspecció signifiqui l'accés de l'administrador al contingut dels correus electrònics".*

En relació amb la possibilitat que l'Ajuntament exerceixi un control, en general, dels sistemes d'informació i, en particular, del correu electrònic dels treballadors que presten serveis públics per a dit consistori, cal fer les consideracions següents.

D'entrada, per tal que es consideri legítim el tractament de dades que pugui derivar del control exercit per l'Ajuntament en aquests casos, cal tenir en compte quina és la finalitat a què respon aquest 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.) perquè 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 l'eliminació dels elements que puguin causar problemes de funcionament dels sistemes d'informació (com ara, virus informàtics, programaris no autoritzats, etc.). En definitiva, són necessàries per assegurar el correcte funcionament dels sistemes d'informació.

D'altra banda, cal tenir present que la jurisprudència ha manifestat que el poder de direcció de l'empresari inclou facultats de control de l'activitat laboral. Pel que fa, en concret, al control de l'ordinador, cal fer necessàriament referència a la Sentència de 26 de setembre de 2007 del Tribunal Suprem, dictada en el recurs de cassació per a la unificació de doctrina núm. 966/2006, la doctrina de la qual es pot fer extensible també al control del correu electrònic.

El Tribunal Suprem 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, atès que a través del mateix el treballador executa la prestació del treball, i considera que l'empresari és el titular del dit ordinador, sigui com a propietari o per altre títol. Per això, dictamina que 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 concret, en aquesta sentència s'estableix, entre d'altres aspectes, que:

"La cuestión debatida se centra, por tanto, en determinar si las condiciones que el artículo 18 del Estatuto de los Trabajadores establece para el registro de la persona del trabajador, su taquilla y sus efectos personales se aplican también al control empresarial sobre el uso por parte del trabajador de los ordenadores facilitados por la empresa. Pero el problema es más amplio, porque, en realidad, lo que plantea el recurso, desde la perspectiva de ilicitud de la prueba obtenida vulnerando los derechos fundamentales (artículo 91.1 de la Ley de Procedimiento Laboral), es la compatibilidad de ese control empresarial con el derecho del trabajador a su intimidad personal (artículo 18.1 de la Constitución o incluso con el derecho al secreto de las comunicaciones (artículo 18.3 de la Constitución Española), si se tratara del control del correo electrónico. El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos establece también que toda persona tiene derecho al respeto de la vida privada y familiar y prohíbe la injerencia que no esté prevista en la Ley y que no se justifique por razones de seguridad, bienestar económico, defensa del orden, prevención de las infracciones penales, protección de la salud, de la moral o de los derechos y libertades de los demás. (...)

En el caso del uso por el trabajador de los medios informáticos facilitados por la empresa pueden producirse conflictos que afectan a la intimidad de los trabajadores, tanto en el correo electrónico, en el que la implicación se extiende también, como ya se ha dicho, al secreto de las comunicaciones, como en la denominada «navegación» por Internet y en el acceso a determinados archivos personales del ordenador. Estos conflictos surgen porque existe una utilización personalizada y no meramente laboral o profesional del medio facilitado por la empresa. Esa utilización personalizada se produce como consecuencia de las dificultades prácticas de establecer una prohibición absoluta del empleo personal del ordenador –como sucede también con las conversaciones telefónicas en la empresa- y de la generalización de una cierta tolerancia con un uso moderado de los medios de la empresa. Pero, al mismo tiempo, hay que tener en cuenta que se trata de medios que son propiedad de la empresa y que ésta facilita al trabajador para utilizarlos en el cumplimiento de la prestación laboral, por lo que esa utilización queda dentro del ámbito del poder de vigilancia del empresario, que, como precisa el artículo 20.3 del Estatuto de los Trabajadores, implica que éste «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», aunque ese control debe respetar «la consideración debida» a la «dignidad» del trabajador." (FJ II).

"Tanto la persona del trabajador, como sus efectos personales y la taquilla forman parte de la esfera privada de aquél y quedan fuera del ámbito de ejecución del contrato de trabajo al que se extienden los poderes del artículo 20 del Estatuto de los Trabajadores. Por el contrario, las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el empresario «como propietario o por otro título» y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen. Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el empresario puede verificar en él su correcto cumplimiento, lo que no sucede en los supuestos del artículo 18 (...).

El empresario tiene que controlar el uso del ordenador, porque en él se cumple la prestación laboral y, por tanto, ha de comprobar si su uso se ajusta a las finalidades que lo justifican, ya que en otro caso estaría retribuyendo como tiempo de trabajo el dedicado a actividades extralaborales. Tiene que controlar también los contenidos y resultados de esa prestación (...).

El control de los ordenadores se justifica también por la necesidad de coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencias de los trabajadores (pedidos, relaciones con clientes...), por la protección del sistema informático de la empresa, que puede ser afectado negativamente por determinados usos, y por la prevención de responsabilidades que para la empresa pudieran derivar también algunas formas ilícitas de uso frente a terceros. En realidad, el control empresarial de un medio de trabajo no necesita, a diferencia de lo que sucede con los supuestos del artículo 18 del Estatuto de los Trabajadores, una justificación específica caso por caso. Por el contrario, su legitimidad deriva directamente del artículo 20.3 del Estatuto de los Trabajadores (...)" (FJ III).

Seguint, doncs, aquesta doctrina, es pot afirmar que l'Ajuntament, en la seva condició d'"empresari", a banda de poder dur a terme les tasques de manteniment i revisió que siguin necessàries per assegurar el correcte funcionament dels sistemes d'informació, 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.

Així mateix, també es 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, així com 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.

Dit això, però, 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).

En aquest sentit, el Tribunal Suprem condiciona, en l'esmentada sentència, 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, considera que si l'empresari (en el nostre cas, l'Ajuntament) vol exercir un control dels mitjans informàtics ha d'informar prèviament als treballadors sobre el contingut i abast de dit control:

> *"(…) 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» (…)"* (FJ IV).

En relació amb el cas concret, convé assenyalar que l'Ajuntament amb la comunicació als treballadors del Manual de bones pràctiques que ara s'analitza estaria, precisament, donant compliment a aquest requisit d'informació prèvia als afectats exigit per la jurisprudència.

Ara bé, un cop examinades les previsions d'aquest Manual al respecte, cal fer avinent que seria recomanable oferir una informació més clara, tant pel que fa a l'ús concret que els treballadors poden fer de les TIC, com al fet d'explicar quines seran les mesures concretes de control de les eines de treball -entre elles, del correu electrònic- que puguin afectar la privacitat de les persones, així com les conseqüències que es poden derivar d'aquest control.

Per exemple, convé evitar interpretacions contradictòries sobre quins usos estan permesos i quins no. Els apartats 5.1 i 5.2 del Manual de bones pràctiques estableixen que, amb caràcter general, no està permès l'ús per a fins personals o privats de les eines informàtiques que l'Ajuntament posa a disposició dels seus treballadors. Podria entendre's, per tant, que aquesta prohibició engloba també el correu electrònic facilitat als treballadors. Aquesta assumpció semblaria encertada si es té en compte allò previst a l'annex del Manual, segons el qual els usuaris dels recursos informàtics de l'Ajuntament adquireixen el compromís d'utilitzar, no només Internet, sinó també el correu electrònic *"per motius estrictament i exclusivament professionals, i en cap cas fer-ne un ús privat o particular".* Ara bé, a l'apartat 7.1 del Manual s'indica, precisament, tot el contrari. Segons aquest apartat el correu electrònic pot ser utilitzat de manera *"incidental i ocasional per a propòsits personals"* amb determinades condicions. A més, l'enunciat d'aquest apartat estableix que l'ús del correu electrònic *"ens representa personalment però també com a membres de l'Ajuntament",* afirmació que semblaria indicar l'existència d'un correu electrònic facilitat per l'Ajuntament que pot ser emprat per a fins personals o privats. S'entén, en relació amb aquest darrer aspecte que, en realitat, l'Ajuntament vol indicar que el correu electrònic facilitat els representa o els identifica com a treballadors de l'Ajuntament, per la qual cosa convindria modificar aquest enunciat. Així mateix, caldria facilitar als treballadors una informació més concisa pel que fa a l'ús del correu electrònic que no indueixi a confusions.

En aquest mateix sentit, també seria recomanable facilitar una informació més concreta en l'apartat 7.3 del Manual de bones pràctiques, relatiu al control dels missatges de correu electrònic, quins supòsits, a banda del ja previst, podrien donar lloc a aquest control (per exemple, per dur a terme tasques de manteniment del sistema d'informació, per garantir la continuïtat laboral en cas d'absència imprevista, etc.) i quines en poden ser les conseqüències.

Dit això, es considera que les previsions dels apartats 2.3 i 7.3 del Manual de bones pràctiques (i de l'annex) no són contràries a la normativa de protecció de dades, si bé seria recomanable millorar-ne la seva redacció actual per tal de facilitar una informació més clara i precisa als treballadors de l'Ajuntament.

V

El sindicat també manifesta que diverses previsions del Manual de bones pràctiques relacionades amb les mesures de seguretat aplicables podrien no adequar-se a la normativa de protecció de dades.

En aquest sentit, assenyala les previsions dels apartats 1.3, 3.4, 5.4 i 6 del Manual, relatives a la compartició d'equipaments informàtics o d'espais d'emmagatzematge i als mecanismes d'identificació i d'autentificació, així com les previsions dels apartats 8.11.1 i 8.12 del Manual, atès que considera que no permeten conèixer amb suficient claredat quines mesures de seguretat en concret s'han de tenir en compte en el tractament de dades personals.

En relació amb aquest aspecte, convé tenir en compte, d'entrada, que la normativa de protecció de dades personals imposa l'obligació al responsable del tractament (en aquest cas, l'Ajuntament) i, si s'escau, a l'encarregat del tractament d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries per tal de garantir la seguretat de les dades personals que seran tractades, així com per evitar la seva alteració, pèrdua, tractament o accés no autoritzat (article 9 LOPD).

Aquestes mesures de seguretat venen regulades en el Títol VIII del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la LOPD (RLOPD), que les classifica en tres nivells diferents –bàsic, mitjà i alt- en funció de la tipologia de dades personals que en cada cas es prevegin tractar. Cal tenir en compte, que aquestes mesures tenen un caràcter acumulatiu, de tal manera que les establertes per a cada nivell exigeixen incorporar les previstes per als nivells inferiors.

L'article 81 del RLOPD estableix, en relació amb l'aplicació dels nivells de seguretat, el següent:

"1. Tots els fitxers o tractaments de dades de caràcter personal han d'adoptar les mesures de seguretat qualificades de nivell bàsic.
2. S'han d'implantar, a més de les mesures de seguretat de nivell bàsic, les mesures de nivell mitjà, en els següents fitxers o tractaments de dades de caràcter personal:
a) Els relatius a la comissió d'infraccions administratives o penals.
b) Aquells el funcionament dels quals es regeixi per l'article 29 de la Llei orgànica 15/1999, de 13 de desembre.
c) Aquells els responsables dels quals siguin administracions tributàries i es relacionin amb l'exercici de les seves potestats tributàries.
d) Aquells els responsables dels quals siguin les entitats financeres per a finalitats relacionades amb la prestació de serveis financers.
e) Aquells els responsables dels quals siguin les entitats gestores i serveis comuns de la Seguretat Social i es relacionin amb l'exercici de les seves competències. De la

mateixa manera, aquells els responsables dels quals siguin les mútues d'accidents de treball i malalties professionals de la Seguretat Social.
f) Els que continguin un conjunt de dades de caràcter personal que ofereixin una definició de les característiques o de la personalitat dels ciutadans i que permetin avaluar determinats aspectes de la seva personalitat o comportament.
3. A més de les mesures de nivell bàsic i mitjà, les mesures de nivell alt s'han d'aplicar en els següents fitxers o tractaments de dades de caràcter personal:
a) Els que es refereixin a dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual.
b) Els que continguin o es refereixin a dades obtingudes per a fins policials sense consentiment de les persones afectades.
c) Els que continguin dades derivades d'actes de violència de gènere.
4. Als fitxers els responsables dels quals siguin els operadors que prestin serveis de comunicacions electròniques disponibles al públic o explotin xarxes públiques de comunicacions electròniques respecte a les dades de tràfic i a les dades de localització, s'hi han d'aplicar, a més de les mesures de seguretat de nivell bàsic i mitjà, la mesura de seguretat de nivell alt que conté l'article 103 d'aquest Reglament.
5. En el cas de fitxers o tractaments de dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual només s'han d'implantar les mesures de seguretat de nivell bàsic quan:
a) Les dades s'utilitzin amb l'única finalitat de realitzar una transferència dinerària a les entitats de què els afectats siguin associats o membres.
b) Es tracti de fitxers o tractaments on de forma incidental o accessòria s'incloguin aquelles dades sense tenir relació amb la seva finalitat.
6. També es poden implantar les mesures de seguretat de nivell bàsic en els fitxers o tractaments que continguin dades relatives a la salut, referents exclusivament al grau de discapacitat o la simple declaració de la condició de discapacitat o invalidesa de l'afectat, amb motiu del compliment de deures públics.
7. Les mesures incloses en cadascun dels nivells descrits anteriorment tenen la condició de mínims exigibles, sense perjudici de les disposicions legals o reglamentàries específiques vigents que puguin ser aplicables en cada cas o les que per pròpia iniciativa adopti el responsable del fitxer.
8. Als efectes de facilitar el compliment del que disposa aquest títol, quan en un sistema d'informació existeixin fitxers o tractaments que, en funció de la seva finalitat o ús concret, o de la naturalesa de les dades que continguin, requereixin l'aplicació d'un nivell de mesures de seguretat diferent que el del sistema principal, es poden segregar d'aquest últim, i és aplicable en cada cas el nivell de mesures de seguretat corresponent i sempre que es puguin delimitar les dades afectades i els usuaris que hi tinguin accés, i que això es faci constar en el document de seguretat."

D'acord amb aquest precepte, atès que, en aquest cas, l'Ajuntament, en exercici de les seves competències, pot tractar, tal i com s'ha posat de manifest anteriorment, informació de diversa índole i, per tant, fins i tot, informacions de caràcter sensible (com ara, a tall d'exemple, ideologia, afiliació sindical, salut, vida sexual, etc.), les mesures de seguretat que haurà d'implementar seran, a més de les mesures de nivell bàsic i mitjà, les mesures de nivell alt (article 81.3.a) RLOPD).

En concret, tenint en compte que el tractament de dades s'efectuarà de manera automatitzada, caldrà aplicar les mesures descrites en els articles 89 a 104 del RLOPD, consistents en:

a) L'elaboració d'un document de seguretat on es fixin les obligacions i funcions dels usuaris o perfils d'usuaris que accedeixin a les dades, una descripció del sistema informàtic i una definició de les funcions de control o autoritzacions delegades pel responsable del fitxer o tractament (article 89 RLOPD).

b) L'establiment d'un registre d'incidències (articles 90 i 100 RLOPD).
c) L'establiment d'un control d'accés (article 91 RLOPD).
d) La correcta gestió de suports i documents (articles 92, 97 i 101 RLOPD).
e) L'adopció de mesures que garanteixin la correcta identificació i autenticació dels usuaris (articles 93 i 98 RLOPD).
f) L'establiment de processos de còpies de seguretat i recuperació de les dades (articles 94 i 102 RLOPD).
g) L'assignació d'un o diversos responsables de seguretat (article 95 RLOPD).
h) La realització d'auditories de seguretat (article 96 RLOPD).
i) L'establiment d'un control d'accés físic (article 99 RLOPD).
j) L'establiment d'un registre d'accessos (article 103 RLOPD).
k) L'establiment de mecanismes de xifratge, en cas de transmissió de les dades a través de xarxes públiques o xarxes sense fil de comunicacions electròniques (article 104 RLOPD).

L'Ajuntament té, per tant, l'obligació de vetllar pel compliment d'aquestes mesures de seguretat. Ara bé, tenint en compte que la seva implementació requereix, en major o menor mesura, la implicació directa dels usuaris, pot afirmar-se que l'Ajuntament també té l'obligació 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 a seguir. És a dir, qualsevol usuari del sistema d'informació ha d'estar assabentat de com ha gestionar els diferents elements que el conformen.

En el cas plantejat, les previsions en relació amb les mesures de seguretat que s'implementaran les trobem, majoritàriament, a l'apartat 8 del Manual de bones pràctiques, si bé és cert que al llarg de tot el text també hi trobem altres referències en aquest sentit (per exemple, en els apartats 3, 5 o 6). Per tant, es pot deduir que l'objectiu del Manual sobre el qual es demana el parer de l'Autoritat és, precisament, informar els usuaris i concretar els usos correctes dels sistemes d'informació per part d'aquests, en relació amb les seves funcions.

En aquest sentit, es considera que el Manual de bones pràctiques és, amb caràcter general, respectuós amb la normativa de protecció de dades, atès que dóna compliment a les obligacions de l'Ajuntament previstes en la normativa de protecció de dades en relació amb la gestió dels sistemes d'informació.

Ara bé, també és cert que algunes de les previsions actuals del Manual podrien resultar massa generals o, si més no, poc precises per als usuaris dels sistemes d'informació, tal i com assenyala el sindicat en el seu escrit de consulta. Per exemple, l'apartat 8.12 estableix que s'han de respectar les mesures de seguretat que adopti l'Ajuntament per tal de garantir la confidencialitat i integritat de la informació sense més concreció.

Per aquest motiu, seria recomanable establir, en un apartat específic del Manual de bones pràctiques, el conjunt de mesures de seguretat que, en concret, cal tenir en compte en aquest sentit, de conformitat amb allò previst al RLOPD, ja siguin de caràcter més general o respecte aspectes més concrets (com ara, en relació amb l'ús del correu electrònic). Més enllà de fer una relació completa d'aquestes mesures de seguretat o del contingut del document de seguretat en aquest Manual, es tractaria, en qualsevol cas, de garantir-ne el seu coneixement per part de tots usuaris del sistema d'informació de l'Ajuntament.

En relació amb aquelles altres observacions relacionades amb les mesures de seguretat que, en concret, fa el sindicat en el seu escrit de consulta, convé apuntar que:

- L'apartat 1.3 del Manual de bones pràctiques estableix que cal deixar *"cada dia els equips informàtics en el millor estat de disponibilitat, ordre i neteja per tal que les persones que puguin venir després els trobin tal com a vosaltres us agradaria trobar-los".*

S'entén, d'aquestes previsions, que aquests equips informàtics podran ser d'ús compartit entre els treballadors municipals. Tal previsió no comporta cap problema des del punt de vista del dret a la protecció de dades personals sempre que es garanteixi que cada treballador tindrà accés només als recursos que necessiti per a l'exercici de les seves funcions (article 91 RLOPD). En aquest sentit, cal fer esment tant a l'apartat 5.4, que preveu precisament aquest extrem, com a l'apartat 6, que preveu l'ús d'usuaris i contrasenyes com a mecanisme d'identificació i d'autenticació per accedir als recursos informàtics de l'Ajuntament. Tenint en compte, doncs, aquestes previsions, l'apartat 1.3 del Manual es considera correcte.

- L'apartat 3.4 del Manual de bones pràctiques estableix que cal treballar *"en discos de xarxa i amb bústies departamentals sempre que els mètodes de treball i procediments del vostre servei ho permeti. La utilització d'espais comuns d'emmagatzematge evita la duplicitat d'informació i facilita les còpies de seguretat*".

En relació amb aquesta previsió es fa extensible la consideració feta anteriorment, en el sentit que no resulta contrària a la normativa de protecció de dades, atesa la previsió en el mateix Manual (apartats 6 i 8) d'adoptar les mesures de seguretat escaients, per tal de garantir que cada usuari tingui accés als recursos a què estigui autoritzat.

- L'apartat 5.4 del Manual de bones pràctiques preveu, com s'ha avançat, que *"cada lloc de treball únicament ha de tenir accés als recursos als quals hi està autoritzat"*.

Aquesta previsió concorda amb la mesura de seguretat de l'article 91 del RLOPD relativa a l'establiment d'un control d'accés que, obligatòriament, ha d'implementar el responsable del tractament de dades personals (l'Ajuntament), per la qual cosa es considera correcta. Aquest article del RLOPD estableix, en concret, que:

> *"Article 91. Control d'accés*
> *1. Els usuaris han de tenir accés només als recursos que necessitin per a l'exercici de les seves funcions.*
> *2. El responsable del fitxer s'ha d'encarregar que hi hagi una relació actualitzada d'usuaris i perfils d'usuaris, i els accessos autoritzats per a cadascun d'ells.*
> *3. El responsable del fitxer ha d'establir mecanismes per evitar que un usuari pugui accedir a recursos amb drets diferents dels autoritzats.*
> *4. Exclusivament el personal autoritzat per fer-ho en el document de seguretat pot concedir, alterar o anul·lar l'accés autoritzat sobre els recursos, de conformitat amb els criteris que estableix el responsable del fitxer.*
> *5. En cas que existeixi personal aliè al responsable del fitxer que tingui accés als recursos, ha d'estar sotmès a les mateixes condicions i obligacions de seguretat que el personal propi."*

Dit això, escau recordar que, en cas que l'Ajuntament dugui a terme el tractament de dades que requereixin l'adopció d'un nivell alt de seguretat, també haurà d'implementar un registre d'accessos, de conformitat amb allò establert a l'article 103 del RLOPD:

> *"Article 103. Registre d'accessos*
> *1. De cada intent d'accés s'han de guardar, com a mínim, la identificació de l'usuari, la data i hora en què es va realitzar, el fitxer a què s'ha accedit, el tipus d'accés i si ha estat autoritzat o denegat.*

2. En cas que l'accés hagi estat autoritzat, és necessari guardar la informació que permeti identificar el registre a què s'ha accedit.
3. Els mecanismes que permeten el registre d'accessos han d'estar sota el control directe del responsable de seguretat competent sense que hagin de permetre la seva desactivació ni manipulació.
4. El període mínim de conservació de les dades registrades és de dos anys.
5. El responsable de seguretat s'ha d'encarregar de revisar almenys una vegada al mes la informació de control registrada i ha d'elaborar un informe de les revisions realitzades i els problemes detectats.
6. No és necessari el registre d'accessos definit en aquest article en cas que es donin les circumstàncies següents:
a) Que el responsable del fitxer o del tractament sigui una persona física.
b) Que el responsable del fitxer o del tractament garanteixi que únicament ell té accés a les dades personals i les tracta.
La concurrència de les dues circumstàncies a què es refereix l'apartat anterior s'ha de fer constar expressament en el document de seguretat."

Aquesta mesura de seguretat, a més, pot ser recomanable si els equips informàtics són d'ús compartit.

- L'apartat 6 del Manual de bones pràctiques fa referència, entre d'altres aspectes, als mecanismes d'identificació i d'autenticació emprats per l'Ajuntament per garantir l'accés correcte dels treballadors als recursos informàtics, que estan basats en l'ús d'usuaris i contrasenyes.

Aquesta previsió resulta conforme amb allò previst a l'article 93 del RLOPD, si bé cal que l'Ajuntament tingui en compte que:

- El procediment de gestió de les contrasenyes ha de garantir la confidencialitat i la integritat de les mateixes.
- La contrasenya ha de ser robusta. La major o menor exigència en aquest aspecte dependrà de la naturalesa de la informació protegida, però en qualsevol cas pot portar a establir uns requeriments mínims.
- Les contrasenyes s'han de canviar de forma periòdica, i en qualsevol cas sempre abans d'un any. Així mateix, mentre estiguin vigents, s'han d'emmagatzemar de forma inintel·ligible.
- Ha d'establir perfils d'usuaris per tal que cada usuari pugui accedir només a aquella informació per a la qual estigui autoritzat.

A més, escau recordar que, en cas que es dugui a terme un tractament de dades que requereixin l'adopció d'un nivell mitjà de seguretat, també haurà d'establir un mecanisme que limiti la possibilitat d'intentar reiteradament l'accés no autoritzat al sistema d'informació, tal i com estableix l'article 98 del RLOPD.

- Pel que fa a la menció que es fa en l'apartat 8.3 del Manual de bones pràctiques al Reial decret 994/1999, d'11 de juny, pel qual s'aprova el Reglament de mesures de seguretat dels fitxers automatitzats que continguin dades de caràcter personal, en tractar-se d'una norma derogada pel Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la LOPD, tal i com apunta el sindicat en el seu escrit, caldrà modificar-la.

VI

En relació amb aquelles altres observacions fetes pel sindicat al seu escrit de consulta de caràcter més general, es fan les consideracions següents.

D'una banda, s'assenyala que la previsió de l'apartat 5.6 del Manual de bones pràctiques, relativa al secret professional, no pot emparar fets delictius de l'Ajuntament relacionats amb les dades de caràcter personal, la utilització de les xarxes o els serveis informàtics.

Més enllà del fet que això sigui cert, cal fer avinent que, des de la vessant del dret a la protecció de dades personals, l'Ajuntament, com a responsable, així com totes aquelles persones que intervinguin en qualsevol fase del tractament de les dades personals (com ara, els usuaris dels sistemes d'informació o els treballadors municipals) estan obligats al secret professional "*pel que fa a les dades i al deure de guardar-les, obligacions que subsisteixen fins i tot després de finalitzar les seves relacions amb el titular del fitxer o, si s'escau, amb el seu responsable"* (article 10 LOPD).

D'altra banda, s'assenyala que l'apartat 8.6 del Manual de bones pràctiques podria no adequar-se a la normativa de protecció de dades, atesa la previsió de l'Ajuntament d'establir que *"qui creï fitxers que continguin dades de caràcter personal o desenvolupi aplicacions o programes que les tractin al marge del Servei d'Informàtica serà el responsable del fitxer o tractament amb les conseqüències legals que se'n derivin".*

D'entrada, cal fer avinent que l'Ajuntament empra incorrectament el terme "fitxer de dades personals" a l'hora de referir-se, com així sembla ser, a la possible creació de bases de dades, carpetes o arxius en què es pugui emmagatzemar informació personal per part dels treballadors.

És clar que quan l'exercici de les funcions de les administracions públiques comporta la recollida i el tractament estructurat de dades personals, ja sigui de forma automatitzada o no, s'ha de crear el corresponent fitxer, entès com *"qualsevol conjunt organitzat de dades de caràcter personal, sigui quina sigui la forma o la modalitat de creació, emmagatzematge, organització i accés"* (article 3.b) LOPD), abans d'iniciar la recollida de dades i que, en el cas examinat, aquesta obligació recau sobre l'Ajuntament, que és el responsable d'aquests tractaments, a través de l'aprovació d'una disposició de caràcter general (ordenança o reglament del ple de la corporació) amb els apartats exigits pels articles 20 de la LOPD i 54 del RLOPD.

Dit això, cal tenir present que les dades personals recollides per l'Ajuntament només poden ser sotmeses a tractament 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 (article 4.1 LOPD). És a dir, les dades no poden utilitzar-se per a finalitats incompatibles amb aquelles per a les quals hagin estat recollides (article 4.2 LOPD).

A aquesta prohibició semblaria referir-se, precisament, l'Ajuntament en aquest apartat 8.6 del Manual de bones pràctiques. Els treballadors municipals no poden emprar les dades personals obtingudes per l'Ajuntament, de conformitat amb l'article 6.2 de la LOPD, en exercici de les seves competències per crear, posteriorment, les seves pròpies bases de dades, carpetes, arxius o sistemes d'emmagatzematge d'informació anàlegs i destinar aquestes dades per a altres finalitats diferents a les que varen justificar la seva recollida.

En el cas que els treballadors procedeixin a la creació d'aquestes bases de dades, carpetes o arxius amb informació personal per a finalitats privades –suposem que la previsió s'està referint a aquest supòsit-, és cert que, com preveu l'Ajuntament al Manual, seran considerats responsables del tractament o fitxer i, per tant, els resultarà aplicable el règim sancionador previst a la LOPD.

Altra cosa és que, en relació amb aquells fitxers i tractaments dels que és responsable l'Ajuntament, una actuació incorrecta o contrària a les previsions de la LOPD, del RLOPD o a les instruccions donades per aquest en el Manual de bones pràctiques, per part dels

seus empleats també pugui comportar la depuració de les corresponents responsabilitats per part del propi Ajuntament.

Ateses aquestes consideracions, es recomana, en qualsevol cas, modificar la redacció actual de l'apartat 8.6 del Manual de bones pràctiques, per tal que resulti més clara i precisa.

També s'assenyala que l'apartat 8.9 del Manual de bones pràctiques podria no adequar-se a la normativa de protecció de dades, atesa la previsió de l'Ajuntament de que cada treballador hagi de consultar els seus responsables en cas de ser necessària la comunicació o cessió de dades personals.

En relació amb aquest aspecte, el RLOPD estableix que *"la sortida de suports i documents que continguin dades de caràcter personal, inclosos els compresos i/o annexos a un correu electrònic, fora dels locals sota el control del responsable del fitxer o tractament, l'ha d'autoritzar el responsable del fitxer o ha d'estar degudament autoritzada en el document de seguretat"* (article 92.2).

Així mateix, preveu que *"les autoritzacions que en aquest títol s'atribueixen al responsable del fitxer o tractament poden ser delegades en les persones designades a aquest efecte. En el document de seguretat hi han de constar les persones habilitades per atorgar aquestes autoritzacions, així com aquelles en les quals recau la delegació esmentada. En cap cas aquesta designació suposa una delegació de la responsabilitat que correspon al responsable del fitxer"* (article 84).

Per tant, l'Ajuntament, com a responsable, ha d'autoritzar les comunicacions de dades personals o pot delegar aquesta potestat a la persona que designi en el document de seguretat, per exemple, el responsable de cada àrea o unitat del consistori. Més enllà d'aquesta obligació legal, l'Ajuntament pot, si així ho considera convenient, establir altres procediments amb la finalitat de garantir una actuació dels seus treballadors respectuosa amb el dret a la protecció de dades personals.

D'acord amb les consideracions fetes fins ara en relació amb la consulta plantejada, es fan les següents,

Conclusions

Les dades de caràcter personal que tracta l'Ajuntament en aplicació del Manual de bones pràctiques de l'usuari dels recursos informàtics de la Corporació objecte de consulta es troben sotmeses a la normativa de protecció de dades de caràcter personal.

Analitzades, des del punt de vista de la protecció de dades, les previsions del Manual de bones pràctiques esmentat, aquestes no es consideren contràries a la normativa de protecció de dades personals, si bé caldria revisar-les per tal d'oferir una informació més clara i entenedora als treballadors municipals.

Barcelona, 14 de febrer de 2013