Dictamen en relació amb la consulta plantejada per un sindicat sobre l'adequació del Manual d'ús dels sistemes d'informació i comunicació d'una administració pública a la normativa de protecció de dades

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit emès per un sindicat, en què se sol·licita a l'Autoritat l'emissió d'un dictamen sobre l'adequació del Manual d'ús dels sistemes d'informació i comunicació d'una administració pública a la normativa de protecció de dades.

Atès que a l'escrit en el qual es formula la consulta no es va adjuntar l'esmentat Manual d'ús dels sistemes d'informació i comunicació, es va requerir l'entitat consultant per tal que n'aportés un exemplar actualitzat.

Analitzada la petició i la documentació aportada arran del requeriment, vista la normativa vigent aplicable, i vist l'informe de l'Assessoria Jurídica emeto el següent dictamen.

I

(...)

II

En l'escrit de consulta s'exposa que l'administració pública disposa d'un Manual d'ús dels sistemes d'informació i comunicació (en endavant, el Manual d'ús), adreçat al col·lectiu de treballadors de l'entitat, l'entrada en vigor del qual va tenir lloc el passat mes de gener.

Tot seguit, afegeix que algunes previsions d'aquest Manual d'ús 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.

Les previsions assenyalades en l'escrit de consulta fan referència als aspectes següents:

a) L'establiment d'un registre d'accessos a Internet per part de l'administració (article 9.6).
b) La responsabilitat dels treballadors públics en l'ús de xarxes socials, xats i fòrums en nom de l'administració (article 10).
c) La utilització del correu electrònic corporatiu pels treballadors públics amb fins personals (article 11).
d) Les conseqüències de l'incompliment de les previsions establertes en el Manual d'ús per als treballadors públics (article 20).

Aquestes qüestions s'analitzen, a continuació, des del punt de vista del dret a la protecció de les dades personals (article 18.4 CE), que és la perspectiva des de la qual s'emet aquest dictamen. Convé assenyalar, per tant, que no correspon a aquesta Autoritat informar sobre la pertinença, l'abast o el contingut d'altres aspectes del Manual d'ús.

III

El Manual d'ús que s'examina té per objecte *"establir els criteris generals i les normes d'ús que s'han d'observar per a l'adequada utilització de les TIC que la (...), com a titular i/o proveïdor, posa a disposició del personal que hi presta serveis, independentment de la relació jurídica que el vinculi a la corporació",* així com *"garantir l'ús correcte de les eines de treball i la infraestructura tecnològica"* (article 1.1).

En l'escrit de consulta s'assenyala, d'entrada, que les previsions de l'article 9.6 del Manual d'ús, emmarcat en les normes relatives a l'accés a Internet per part dels treballadors de la corporació, podrien no adequar-se a la normativa de protecció de dades.

Aquest article estableix que *"la (...) registrarà, en els termes establerts en el Reial decret 3/2010, de 8 de gener, que regula l'esquema nacional de seguretat en l'àmbit de l'Administració electrònics i normativa concordant, els accessos, incloent-hi, com a mínim, la següent informació: les adreces de les pàgines visitades, data i hora, fitxers descarregats i l'usuari o lloc des d'on s'ha fet la connexió."*

Des del punt de vista de la protecció de dades personals, qualsevol tractament d'informació personal requereix el consentiment inequívoc de l'afectat o, en el seu defecte, una llei o norma amb rang de llei que l'habiliti (article 6.1 de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, LOPD)).

En aquest sentit, la mateixa LOPD estableix que aquest consentiment no és necessari quan, entre d'altres supòsits, les dades de caràcter personal *"es refereixin a les parts d'un contracte o un precontracte d'una relació de negoci, laboral o administrativa i siguin necessàries per al seu manteniment o compliment"* (article 6.2).

Per tant, convé assenyalar que la legitimació per als tractaments de dades dels treballadors a què es refereix el present Manual d'ús i, en particular, aquest article 9.6, per part de l'administració deriva de l'existència d'una relació laboral o estatutària entre aquests treballadors i la dita corporació, relació que s'haurà de desenvolupar de conformitat amb la normativa que li resulti d'aplicació.

Dit això, convé tenir en compte que la normativa de protecció de dades personals imposa l'obligació al responsable del tractament (en aquest cas, l'administració) 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.

Més enllà del compliment de les previsions del RLOPD, citat, l'administració també haurà de donar compliment a allò disposat en el Reial decret 3/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica (en endavant, ENS), que resulta d'aplicació a totes les Administracions públiques en els

termes de l'article 2 de la Llei 7/2011, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

L'ENS preveu una avaluació de riscos i l'aprovació d'una política de seguretat, a partir de la qual s'establirà una categorització dels sistemes d'informació i es determinaran les mesures de seguretat concretes a aplicar en cada cas. Aquestes previsions són d'aplicació tant a la informació relativa a persones físiques com a persones jurídiques.

En concret, l'article 1 de l'esmentat Reial decret 3/2010 estableix que:

> *"1. El present Reial decret té per objecte regular l'Esquema Nacional de Seguretat que estableix l'article 42 de la Llei 11/2007, de 22 de juny, i determinar la política de seguretat que s'ha d'aplicar en la utilització dels mitjans electrònics a què es refereix la Llei esmentada.*
> *2. L'Esquema Nacional de Seguretat està constituït pels principis bàsics i requisits mínims requerits per a una protecció adequada de la informació. És aplicat per les administracions públiques per assegurar l'accés, integritat, disponibilitat, autenticitat, confidencialitat, traçabilitat i conservació de les dades, informacions i serveis utilitzats en mitjans electrònics que gestionin en l'exercici de les seves competències."*

L'ENS conté diverses referències a la supervisió i el control del personal de les Administracions públiques com a usuari de llurs sistemes d'informació, per tal de garantir-ne la seguretat. Als efectes que interessen convé destacar-ne les següents:

L'article 14, relatiu a la gestió de personal, segons el qual:

> *"1. Tot el personal relacionat amb la informació i els sistemes ha de ser format i informat dels seus deures i obligacions en matèria de seguretat. Les seves actuacions han de ser* ***supervisades*** *per verificar que se segueixen els procediments establerts.*
> *2. El personal relacionat amb la informació i els sistemes ha d'exercir i aplicar els principis de seguretat en l'exercici de la seva feina.*
> *3. El significat i l'abast de l'ús segur del sistema s'ha de concretar i plasmar en unes normes de seguretat.*
> *4. Per corregir, o exigir responsabilitats si s'escau,* ***cada usuari que accedeixi a la informació del sistema ha d'estar identificat de forma única****, de manera que se sàpiga, en tot moment, qui rep drets d'accés, de quin tipus són, i qui ha realitzat determinada activitat."*

L'article 16, relatiu a l'autorització i control d'accessos, segons el qual:

> *"L'accés al sistema d'informació ha de ser* ***controlat i limitat*** *als usuaris, processos, dispositius i altres sistemes d'informació, degudament autoritzats, restringint l'accés a les funcions permeses."*

I, especialment, l'article 23, relatiu al registre d'activitat, segons el qual:

> *"Amb la finalitat exclusiva d'aconseguir el compliment de l'objecte del present Reial decret, amb plenes garanties del dret a l'honor, a la intimitat personal i familiar i a la mateixa imatge dels afectats, i d'acord amb la normativa sobre protecció de dades personals, de funció pública o laboral, i altres disposicions que siguin aplicables, s'han de* ***registrar les activitats dels usuaris****, i retenir la informació necessària per monitorar, analitzar, investigar i documentar activitats*

indegudes o no autoritzades, i permetre identificar en cada moment la persona que actua."

S'entén que l'article 9.6 del Manual d'ús que s'examina estaria fent referència precisament a aquesta mesura de seguretat de l'ENS.

De conformitat amb les previsions de l'ENS esmentades, l'administració, en el marc de la garantia de la seguretat dels seus sistemes d'informació, estaria legitimada per dur a terme actuacions de supervisió i control de les activitats dutes a terme per les persones usuàries dels dits sistemes.

L'article 2 del Manual d'ús estableix que les normes en ell contingudes s'aplicaran a totes les persones que hagin d'accedir als sistemes d'informació i xarxes de comunicació que siguin propietat o estiguin sota la supervisió de l'administració i que, a tal efecte, tindran la condició d'usuaris.

En la mesura, per tant, que els treballadors de l'administració siguin usuaris dels sistemes d'informació de què disposa la corporació, aquesta podria supervisar i controlar les activitats que, com a tals, realitzen, per tal de verificar que s'ajusten als drets d'accés o autoritzacions de què disposen en atenció a les funcions encomanades i, en darrera instància, per tal de garantir una protecció adequada de la informació i dels seus sistemes, tal com li exigeix la normativa examinada.

Ara bé, la dita supervisió, en la mesura que implicaria el tractament d'informació personal dels treballadors, hauria de ser respectuosa amb el principi de qualitat de les dades, segons el qual *"les dades de caràcter personal només es poden recollir per ser tractades, així com sotmetre-les a aquest 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).

L'esmentat article 23 de l'ENS no concreta la informació personal que, amb fins de garantir la seguretat dels sistemes i de la informació, ha de recollir l'administració pública, si bé estableix que aquesta informació ha de ser la necessària per permetre identificar en cada moment la persona usuària que actua i les activitats indegudes o no autoritzades que es duguin a terme.

En el present cas, l'administració estableix, en l'esmentat article 9.6, que recollirà, com a mínim, la informació sobre els accessos a Internet relativa a les adreces de les pàgines visitades (no el seu contingut), a la data i hora de l'accés, als fitxers descarregats i a l'usuari i lloc des d'on s'ha fet la connexió.

En la mesura que la finalitat perseguida sigui garantir la seguretat dels seus sistemes d'informació, atès que aquesta es podria veure compromesa per la utilització d'Internet, i corregir determinades situacions, així com, si escau, exigir responsabilitats, la informació detallada en aquest article del Manual d'ús podria resultar la necessària per al compliment de tal finalitat.

Ara bé, sent així, caldria eliminar la previsió d'enregistrar "com a mínim" la informació esmentada o, si escau, detallar quina altra informació seria enregistrada amb la finalitat indicada, als efectes de poder establir si el seu tractament s'adequaria al principi de qualitat de dades, citat. Per altra banda, seria recomanable també que es preveiés un termini de conservació d'aquesta informació, que no excedís del termini necessari per a dur a terme aquesta tasca de control.

Sens perjudici d'aquesta observació, i de les consideracions que es faran en el següent fonament jurídic, es considera que les previsions de l'article 9.6 del Manual d'ús poden ser adequades a la normativa de protecció de dades.

IV

En relació amb el control que l'administració pot exercir sobre les eines informàtiques posades a disposició del personal al seu servei als efectes de verificar el compliment de llurs obligacions laborals, convé fer especial 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, relativa al control de l'ordinador per l'empresari, es pot fer extensible també al control del correu electrònic o dels accessos a Internet.

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'administració, 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, així com la seguretat d'aquests sistemes, 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'administració podria realitzar actuacions de control de l'ordinador dels seus treballadors per tal de verificar el compliment d'aquest deure.

Així mateix, 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 CE), però també pel dret a la protecció de dades personals (article 18.4 CE) i pel dret al secret de les comunicacions (article 18.3 CE).

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 citat principi de qualitat, segons el qual, recordem, 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 (article 4 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'administració) 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 el mateix sentit, cal fer referència a la Sentència del Tribunal Constitucional 170/2013, de 7 d'octubre, que també admet el control empresarial sobre les eines informàtiques analitzant si existeix o no "*una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas".* En

aquest supòsit concret, el conveni col·lectiu contenia una previsió expressa d'ús exclusiu professional, incloent un tipus sancionador al respecte, per la qual cosa es va considerar que el treballador no podria tenir tal expectativa de privacitat o confidencialitat, sent el control exercit per l'empresari, per tant, lícit (FJ V).

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

Respecte a l'ús de les eines de treball i la infraestructura tecnològica per part dels treballadors de l'administració, el Manual d'ús és clar en establir que, en general, aquestes eines s'han de destinar exclusivament per al desenvolupament de les tasques i funcions encomanades (article 4).

Pel que fa, en concret, a la utilització del maquinari i l'accés a Internet (articles 5 i 9 del Manual d'ús, respectivament), així com pel que fa a l'ús de dispositius mòbils i a l'ús de les TIC per personal extern a l'administració (articles 14 i 18 del Manual d'ús, respectivament), el Manual d'ús també és clar en establir que s'han d'emprar amb finalitats professionals i exclusivament per a l'exercici de les tasques i activitats que corresponen a les funcions del lloc de treball de què es tracti. En relació amb l'accés a Internet, a més, incorpora la previsió de realitzar controls d'accessos per motius de seguretat i de rendiment de la xarxa (article 9.4 del Manual d'ús).

Pel que fa, en concret, a la utilització del correu electrònic (aspecte tractat més endavant), el Manual d'ús també estableix un ús professional del mateix pels treballadors de l'administració, si bé, en aquest cas, n'admet un ús personal esporàdic. Així mateix, incorpora les mesures concretes de control d'aquesta eina de treball que poden afectar la privacitat de les persones (article 11 del Manual d'ús).

A la vista d'aquestes previsions, pot considerar-se que el Manual d'ús examinat és, amb caràcter general, respectuós amb la normativa de protecció de dades, atès que dóna als treballadors informació suficient sobre el contingut i abast del control de les eines de treball que l'administració posa a la seva disposició per al desenvolupament de la prestació de treball.

V

En l'escrit de consulta també s'assenyala que les previsions de l'article 10 del Manual d'ús, relatives a l'accés i ús de les xarxes socials, xats i fòrums d'opinió en nom de l'administració, podrien no adequar-se a la normativa de protecció de dades. En concret, el sindicat manifesta que aquest article suposa una *"descàrrega de responsabilitat sobre els treballadors que han de treballar en l'activitat difusora desenvolupada per la (...)".*

Convé fer avinent, d'entrada, que no queda suficientment clar a què s'està fent referència amb aquesta manifestació. L'esmentat article del Manual d'ús estableix un seguit de recomanacions o bones pràctiques en la utilització de les xarxes socials, xats i fòrums corporatius (l'apartat 2.2.6 recorda que en la publicació d'informacions en aquests espais es representa l'administració) per part d'aquells treballadors de l'administració que han d'emprar aquestes eines per a l'exercici de les funcions i activitats que tenen encomanades.

Les dites recomanacions contribueixen a oferir més seguretat i més respecte pels drets de les persones, en especial, als efectes que interessen, pel dret a la protecció de les

dades de caràcter personal, tants dels mateixos treballadors de l'administració com de terceres persones.

Així, per exemple, s'estableixen indicacions sobre no proporcionar informació adreçada únicament a determinats destinataris, sobre no divulgar informació confidencial o sobre no publicar vídeos ni imatges de persones o situacions del lloc de treball no relacionats amb la feina i sense el seu consentiment (apartats 2.3 i 2.6).

Així mateix, de les previsions de l'apartat 2.1 d'aquest article, es desprèn que qualsevol informació o contingut que sigui publicat pel treballador en un d'aquests espais en exercici de les funcions encomanades requereix l'autorització explícita del comandament immediat. No comptar amb aquesta autorització comportaria, segons aquest apartat, que l'usuari assumeixi la responsabilitat de la publicació efectuada i, per tant, de les conseqüències que se'n puguin derivar.

En concret, s'estableix que *"l'accés sense autorització explícita del comandament immediat implica l'assumpció de responsabilitat personal de l'usuari en relació amb les informacions, opinions, i continguts publicats."*

Respecte aquesta previsió, convé fer avinent que, des del punt de vista de la protecció de dades, la publicació d'informació a través de xarxes socials, xats i fòrums d'opinió, en la mesura que inclogui dades personals (article 3.a) LOPD), quedarà sotmesa a la legislació de protecció de dades. La resta d'informacions publicades en aquests espais, per tant, no seran objecte de protecció per la LOPD, per bé que puguin ser-ho per altra normativa aplicable (per exemple, per la Llei orgànica 1/1982, de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar, i a la pròpia imatge).

Als efectes que interessen, convé assenyalar que la difusió d'informació personal en aquests espais requereix, en la mesura que constitueix una cessió de dades (article 3.i) LOPD), el consentiment de l'afectat o, en el seu defecte, l'existència d'una llei o norma amb rang de llei que l'habiliti (article 11 LOPD).

L'incompliment d'aquest règim de comunicació de dades, així com d'altres principis i obligacions en matèria de protecció de dades, comportaria l'aplicació del règim sancionador establert a la LOPD, el qual, de conformitat amb l'article 43 de la LOPD, recau sobre els responsables dels fitxers o tractaments i els encarregats dels tractaments (article 3.d) i g) LOPD).

Per tant, convé tenir present que, exclusivament des de l'òptica de la protecció de dades, de produir-se una difusió il·lícita d'informació personal de què sigui responsable l'administració a través de les xarxes socials, xats i fòrums corporatius, el règim sancionador previst a la LOPD recauria sobre aquesta corporació, com a responsable, malgrat que la infracció comesa fos materialment atribuïble a una persona concreta que presta serveis a l'administració.

Altra cosa és que aquesta o altra actuació incorrecta o contrària a les previsions de la LOPD, del RLOPD o a les instruccions donades per aquest Manual d'ús per part del personal de l'administració també pogués comportar la depuració de les corresponents responsabilitats per part de la mateixa corporació o, si escau, l'exigència de responsabilitat penal o civil.

Dit això, des del punt de vista de la protecció de dades personals, les pautes establertes en aquest article del Manual d'ús cal valorar-les positivament, atès que formarien part de la responsabilitat *in vigilando* que correspon a l'administració i proporcionarien als

treballadors informació suficient sobre les actuacions permeses (i les que no) en la utilització d'aquestes eines de treball.

VI

El sindicat també qüestiona l'adequació a la normativa de protecció de dades de la previsió de l'article 11 del Manual d'ús relativa a no considerar com correu personal la missatgeria sortint o entrant des de dominis fora de la corporació.

L'esmentat article estableix que *"el sistema informàtic, la xarxa interna, el programari i les estacions de treball utilitzats pels treballadors són propietat de la corporació. És per aquest motiu que cap correu electrònic enviat o rebut des dels sistemes informàtics de la (...) pot tenir, com a norma general, la consideració de personal."*

Convé assenyalar que, tot seguit, en el Manual d'ús s'estableix que *"el correu electrònic pot ser utilitzat excepcionalment per a propòsits personals sempre que:*

a) *No signifiqui una despesa important de temps*
b) *No pugui malmetre l'equipament*
c) *No tingui com a objectiu el lucre personal o del seu entorn ni tingui finalitats publicitàries o comercials (spam)*
d) *No es tracti d'enviaments massius*
e) *No es tracti de missatges en cadena o de tipus piramidal*
f) *No s'enviïn continguts expressament prohibits en aquest document*
g) *No afecti el bon funcionament del servei".*

Del conjunt d'aquestes previsions es desprèn que l'administració, en la seva condició d'empresari, està establint les normes de funcionament d'una eina de treball posada a disposició dels seus treballadors per a l'exercici de les funcions encomanades, per tal d'evitar-ne una mala utilització que pugui perjudicar la seguretat de la informació tractada en la corporació i de la qual n'és responsable.

En concret, es desprèn que el correu electrònic corporatiu ha d'ésser emprat pel seu personal amb finalitat professionals, si bé s'admet també un cert ús amb finalitats privades sempre que es respectin les indicacions donades en el mateix Manual.

L'establiment d'aquestes normes permet a les persones treballadores de l'administració conèixer amb seguretat el nivell de confidencialitat que poden esperar en l'ús d'aquesta eina de treball. Per aquest motiu, es considera que les previsions de l'article 11 del Manual d'ús no resulten contràries a la normativa de protecció de dades.

Tot i així, amb l'objectiu sempre de facilitar una informació clara i entenedora sobre aquesta qüestió, seria bo millorar la redacció dels dos paràgrafs reproduïts més amunt, perquè en la redacció actual hi ha una certa contradicció, atès que mentre al paràgraf quart s'afirma categòricament que "*cap correu electrònic*" pot tenir la consideració de personal, en el paràgraf cinquè s'admeten algunes excepcions en les quals sí que podria tenir aquest caràcter.

Per això seria millor afegir expressament en aquest apartat del Manual que l'ús del correu electrònic facilitat per l'administració s'ha de limitar al desenvolupament de les funcions pròpies del lloc de treball i, tot seguit, indicar aquells supòsits en què s'admet un ús personal ocasional.

Sobre aquesta i d'altres qüestions relacionades amb l'ús del correu electrònic, fer avinent que al web de l'Autoritat (www.apdcat.cat) es pot consultar la Recomanació 1/2013, de l'Autoritat Catalana de Protecció de Dades sobre l'ús del correu electrònic en l'àmbit laboral (adreçada a les administracions públiques catalanes i també a totes els altres ens inclosos dins l'àmbit d'actuació de l'Autoritat), així com el Manual de bon ús del correu electrònic (adreçat a totes les persones treballadores d'aquestes entitats).

VII

El sindicat també fa referència en el seu escrit de consulta a l'article 20 del Manual d'ús, el qual preveu que *"davant de qualsevol ús dels elements d'infraestructura TIC que contravingui l'establert en aquest manual, els òrgans competents, sens perjudici d'adoptar les mesures de restricció o de suspensió d'ús que considerin escaients, podran exigir les responsabilitats disciplinàries o de qualsevol altre ordre que se'n derivin d'acord amb la normativa vigent."*

Considera, al respecte, que amb aquesta previsió es vulnera l'article 36 del RLOPD, relatiu al dret d'oposició a les decisions basades únicament en un tractament automatitzat de dades.

Tal com s'ha posat de manifest al llarg del present dictamen, el Manual conté una sèrie de normes i recomanacions sobre el correcte funcionament de les eines de treball posades a disposició dels treballadors de la corporació, informació sobre el control que, si escau i de conformitat amb la legislació aplicable i la jurisprudència existent en la matèria, pot efectuar la corporació sobre aquest ús, així com les conseqüències que per al seu personal pot comportar l'ús indegut d'aquestes eines.

L'establiment d'aquestes normes obeeix a l'exercici de la potestat d'autoorganització que, com a administració pública de caràcter territorial i en el marc de les seves competències, li atorga la normativa de règim local (article 4 de la Llei 7/1985, de 2 d'abril, reguladora de les bases de règim local, i article 8 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).

Pel que fa al tractament de dades personals dels treballadors que es deriva de l'exercici de la potestat de control de l'administració sobre els mitjans tècnics i informàtics, com s'ha vist, no requereix el consentiment dels afectats (article 6.2 LOPD), sent necessari però complir amb el deure d'informació (article 5 LOPD).

Per la seva part, la normativa vigent en matèria de funció pública imposa una sèrie de deures als treballadors de l'administració, com a empleats públics, tals com, entre d'altres, respectar les normes que integren l'ordenament jurídic, obeir les instruccions professionals dictades pels superiors o no utilitzar els recursos i béns públics en benefici propi, vetllant per la seva conservació (articles 52 a 54 EBEP).

L'incompliment d'aquests deures, així com de l'ordenament jurídic, pot donar lloc, tal com s'ha indicat en apartats anteriors d'aquest dictamen, a l'exigència de responsabilitats, entre elles, la disciplinària (article 93 EBEP).

La determinació de la responsabilitat disciplinària i, si escau, la imposició d'una sanció disciplinària requereix la incoació del corresponent procediment disciplinari (article 98 EBEP), en el qual s'han garantir els principis de legalitat, contradicció, audiència i proporcionalitat (article 264 del Decret 214/1990, de 30 de juliol, pel qual s'aprova el Reglament del personal al servei de les entitats locals).

En atenció a aquestes consideracions, és clar que l'administració pot exercir la potestat disciplinària vers el personal al seu servei en cas d'incompliment de les previsions establerts en el Manual d'ús examinat.

Per la seva part, els treballadors de l'administració poden, de conformitat amb la legislació de protecció de dades, exercir els seus drets d'accés, rectificació, cancel·lació i oposició respecte de la informació que s'hagi obtingut mitjançant les mesures de control d'ús implantades per l'administració (articles 15 a 17 LOPD).

Així mateix, poden impugnar els actes administratius o decisions privades que impliquin una valoració dels seus comportaments, l'únic fonament de les quals sigui un tractament automatitzat de dades personals, que ofereixi una definició de les seves característiques o personalitat (article 13 LOPD).

Precisament a aquest dret d'impugnació de valoracions es refereix l'article 36 del RLOPD que esmenta el sindicat. Aquest article, relatiu al dret d'oposició a les decisions basades únicament en un tractament automatitzat de dades, estableix que:

> *"1. Els interessats tenen dret a no quedar sotmesos a una decisió amb efectes jurídics sobre ells mateixos o que els afecti de manera significativa, que es basi únicament en un tractament automatitzat de dades destinat a avaluar determinats aspectes de la seva personalitat, com ara el seu rendiment laboral, crèdit, fiabilitat o conducta.*
> *2. No obstant això, els afectats poden quedar sotmesos a una de les decisions que preveu l'apartat 1 quan aquesta decisió:*
> *a) S'ha adoptat en el marc de la subscripció o execució d'un contracte a petició de l'interessat, sempre que se li atorgui la possibilitat d'al·legar el que estimi pertinent, a fi de defensar el seu dret o interès. En tot cas, el responsable del fitxer ha d'informar prèviament l'afectat, de forma clara i precisa, que s'han d'adoptar decisions amb les característiques que assenyala l'apartat 1 i que ha de cancel·lar les dades en cas que no s'arribi a subscriure finalment el contracte.*
> *b) L'autoritzi una norma amb rang de llei que estableixi mesures que garanteixin l'interès legítim de l'interessat."*

La decisió adoptada sobre l'afectat a què es refereix aquest article del RLOPD, i que donaria lloc al dret d'oposició citat, ha d'estar fonamentada única i exclusivament en la valoració obtinguda del tractament automatitzat de dades personals. Per tant, cal tenir present que si existís un altre tipus de valoració o apreciació per part del responsable, la prohibició del tractament de les dades que estableix la LOPD deixaria d'existir.

Convé apuntar que es tracta de supòsits en què informàticament es pren una decisió o es fa una valoració que afecta l'interessat emprant en aquest sentit algun tipus d'anàlisi automàtic sobre dades personals (com ara, tècniques de *scoring* o de mineria de dades)sense intervenció humana.

En qualsevol cas, amb el reconeixement d'aquest dret el que es pretén és evitar que una decisió perjudicial per a l'afectat es fonamenti exclusivament en una valoració de la seva persona, producte d'una elaboració informàtica (valoració presa per una "màquina").

Es tracta, per tant, d'una situació que difícilment es podria donar en l'adopció d'una sanció disciplinària que, com s'ha dit, requereix la incoació del corresponent procediment disciplinari, en què s'han de practicar les diligències que siguin adequades per a la identificació i la comprovació dels fets i, en particular, les proves que puguin

conduir al seu aclariment i a la determinació de les responsabilitats susceptibles de sanció, garantint, en qualsevol cas, l'audiència de l'interessat.

De fet, la redacció de l'article 20 del Manual, no sembla que en cap moment apunti a una presa de decisions automatitzada en el sentit exposat, per la qual cosa no sembla que hi hagi una contradicció amb l'article 36 del RLOPD.

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

Conclusions

Les previsions de control contingudes en el Manual d'ús dels sistemes d'informació i comunicació de la corporació objecte de consulta poden comportar el tractament de dades de caràcter personal i, en conseqüència, 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 d'ús esmentat a què es fa referència en la consulta, no es consideren contràries a la normativa de protecció de dades personals, en els termes exposats en aquest dictamen.

Barcelona, 1 de setembre de 2015