CNS 39/2021

Dictamen en relació amb la consulta d'un Ajuntament en relació amb l'accés a l'equip local d'un funcionari de l'Ajuntament, als efectes de poder accedir a informació de l'Ajuntament

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'un Ajuntament, en què es demana Dictamen a aquesta Autoritat en relació amb la possibilitat d'accedir a l'equip local que utilitza un funcionari de l'Ajuntament, que es troba en situació de baixa, per poder accedir a informació propietat de l'Ajuntament, a través del seu departament informàtic.

Analitzada la petició, que no s'acompanya de més informació, vista la normativa vigent aplicable i d'acord amb l'informe de l'Assessoria Jurídica, es dictamina el següent.

I

(...)

II

La consulta es refereix a la possibilitat d'accés a l'equip local que utilitza un funcionari de l'Ajuntament, que es troba en situació de baixa, als efectes de poder accedir a documentació de la Regidoria de Participació Ciutadana de l'Ajuntament. La consulta explica que el funcionari "*és l'únic usuari que centralitza aquesta Regidoria, i per tant crea i guarda la documentació."* Segons la consulta, no poder accedir a aquesta informació paralitza i afecta el desenvolupament de les accions de l'Ajuntament, i afegeix que el funcionari en qüestió té un afer disciplinari amb l'Ajuntament, encara pendent de resolució.

La consulta afegeix que els funcionaris de l'Ajuntament varen rebre formació en protecció de dades i se'ls va explicar el protocol de seguretat de l'Ajuntament (entre d'altres, que no es permeten temes personals en les eines de treball de l'Ajuntament, que s'ha comunicat als treballadors la possibilitat d'accessos a totes les eines de control titularitat de l'Ajuntament, i que es preveu que cal guardar tota la documentació en espais habilitats).

En aquest punt, convé fer avinent que, més enllà que les referències fetes en la consulta a alguns apartats del dit protocol serveixin per emmarcar el supòsit plantejat, l'objecte d'aquest informe no és fer una valoració o validació de l'adequació del protocol de l'Ajuntament a la normativa de protecció de dades.

Dit això, la consulta planteja *"**si podem accedir al equip local** en el que desenvolupa les seves funcions un funcionari de l'Ajuntament, als efectes de poder accedir a informació propietat del Ajuntament, a traves del Departament informàtic del Ajuntament, **per les següents finalitats**:*

A) Posar tota la documentació que pugui existir de la Regidoria esmentada en els espais destinats al efecte
B) Garantir la integritat de la documentació donat que no esta en un espai on es fan còpies de seguretat
C) Corroborar si s'està incomplint les mesures de seguretat del Ajuntament, possibilitat que esta comunicada i acceptada pels funcionaris
D) Desbloquejar la paràlisis de la Regidoria, entenent que es una mesura proporcionada i el bé a protegir es major al que es podria perjudicar. Es a dir, el desenvolupament de una Regidoria, -interès general i múltiples afectats- es més important que el accés al equip de una funcionaria, on podria, i recalquem "podria", existir informació personal, a la que en cap cas, volem accedir
E) Que qualsevol actuació sigui escrupolosa amb la possibilitat de trobada de document de caràcter privat, tot i que estan prohibits temes personals en les eines de treball, vetllant i evitant en aquest cas, qualsevol obertura i accés en aquest continguts
F) Que l'accés seria fet per l'Administrador de sistemes extern –informàtic-
G) Si entenen que s'ha de comunicar aquesta acció al afectat, cas que considerin que es pot fer l'accés, tot i que la consulta es fa des de la perspectiva que el afectat no presta el seu consentiment."

Segons la consulta, aquesta es planteja *"des de la perspectiva que l'afectat no presta el seu consentiment."* Tenint en compte això, partint de la premissa que en el cas plantejat l'Ajuntament no disposaria del consentiment del treballador, caldrà veure si concorre alguna de les bases jurídiques de l'article 6.1 RGPD, que permetin considerar lícit el tractament de dades, i en quines condicions.

III

Segons disposa l'article 87 de l'LOPDGDD:

> *"1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.*
>
> *2.* ***El empleador podrá acceder*** *a los contenidos derivados del uso de medios digitales facilitados a los trabajadores* ***a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.***
>
> *3.* ***Los empleadores deberán establecer criterios de utilización*** *de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.*
>
> *El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.*
>
> *Los* ***trabajadores deberán ser informados*** *de los criterios de utilización a los que se refiere este apartado."*

També cal tenir en compte diverses previsions de la normativa d'àmbit laboral, en relació amb la licitud de les mesures de control per part de l'empresari -en aquest cas, una Administració pública-, del compliment per part dels treballadors, de les seves obligacions laborals.

Especialment, l'article 52 de l'Estatut bàsic del treballador públic (EBEP), segons el qual: *"Los empleados públicos deberán desempeñar con diligencia las tareas que tengan asignadas y velar por los intereses generales con sujeción y observancia de la Constitución y del resto del ordenamiento jurídico (...)",* i l'article 20.3 de l'Estatut dels Treballadors (ET), 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 (...)".*

Des de la perspectiva de la normativa de protecció de dades, com es desprèn de l'article 87 de l'LOPDGDD, les finalitats per a les que resultaria lícita la monitorització dels equips que l'empresari posa a disposició dels treballadors, serien, d'una banda, el control del compliment de les obligacions laborals del treballador (en connexió amb les previsions de la normativa laboral), i de l'altra, la de garantir la integritat dels dispositius que utilitzen els treballadors per al desenvolupament de les seves funcions.

En el cas examinat, i segons la informació disponible, l'Ajuntament (responsable del tractament ex. art. 4.7 RGPD), apunta a que la finalitat principal de l'accés a l'equip assignat al funcionari que es troba de baixa seria la d'assegurar la continuïtat de la feina duta a terme des de l'Ajuntament ja que, segons l'Ajuntament, la documentació guardada en l'equip local que utilitza el treballador seria *"essencial per poder seguir amb l'activitat que desenvolupa la Regidoria"*).

Fem notar que les "finalitats" a les que es refereixen les **preguntes A) i D)** de la consulta (*"Posar tota la documentació que pugui existir de la Regidoria en els espais destinats a l'efecte"* i *"Desbloquejar la paràlisi de la Regidoria (...)"*), atesa la informació de què es disposa, sembla que es refereixen o es relacionen amb aquesta finalitat general d'assegurament del compliment de les funcions que es duen a terme des de la Regidoria de l'Ajuntament.

A això cal afegir que la **pregunta B)** *"Garantir la integritat de la documentació donat que no està en un espai on es fan còpies de seguretat",* segons la informació de què es disposa, també es referiria a la finalitat d'accedir a l'equip en qüestió per tal de protegir la documentació de la Regidoria i per tant, per assegurar el treball desenvolupat des de l'Ajuntament.

Com ha admès la jurisprudència (a tall d'exemple, la STC 61/2021, a la que ens remetem), l'empresari pot establir controls sobre l'ús de les eines que posa a disposició dels treballadors. Especialment rellevant és la STEDH, cas Barbulescu, de 5 de setembre de 2017, en què el TEHDH estableix determinats elements que caldria aplicar en aquest context. En síntesi, el TEDH fa referència a la informació que cal donar als treballadors respecte les mesures que pot prendre l'empresari per a supervisar aquestes eines, en particular, les comunicacions dels treballadors; quin és l'abast de la supervisió, o si l'empresari ha valorat l'existència de mesures de control menys intrusives per als treballadors, entre d'altres (apartat 210 de la STEDH de 5 de setembre de 2017, al que ens remetem).

Segons la consulta, el protocol de l'Ajuntament fa referència a que el responsable del tractament *"informa igualmente a los usuarios que se procederán a eventuales controles*

(contenido del PC, correo electrónico, conexiones internet, servidores y softwares contratados) (...).”

Fem avinent que aquesta Autoritat ha dictat la Recomanació 1/2013, sobre l'ús del correu electrònic en l'àmbit laboral (disponible al web www.apdcat.cat), en la que es fan diferents consideracions que resulten d'especial interès en aquest cas, i a la que ens remetem.

En l'apartat III de la Recomanació, referit a l'accés al correu electrònic per part de l'empresa, es fa avinent també que el mitjà i l'abast del control ha de ser proporcionat a la finalitat que es persegueixi, i s'identifiquen els objectius que podrien justificar l'accés, en aquest cas, als equips o altres dispositius que l'empresari posa a disposició dels treballadors, amb la finalitat d'accedir a la documentació de la Regidoria.

En concret, la Recomanació identifica la possibilitat d'accés amb la finalitat de **garantir la continuïtat de l'activitat en absència de la persona treballadora** (vacances, malaltia, etc.), tenint en compte que l'absència d'un treballador, especialment si és de llarga durada, pot comportar problemes per a la continuïtat normal de l'activitat, si no es pot accedir a determinada informació que, en el cas que ens ocupa, es trobaria en l'equip de què disposa el treballador en situació de baixa. Especialment tenint en compte que, segons la consulta, aquest treballador és "*l'únic usuari que centralitza la informació de la Regidoria*", cosa que hauria provocat, sempre segons la consulta, la paràlisi de les funcions dutes a terme per aquesta.

També afegim que, segons es posa de manifest a l'apartat III de la Recomanació -i atès que es desconeix si el protocol de l'Ajuntament ho ha previst-, és recomanable que, quan la intervenció ve justificada per aquesta finalitat d'assegurar la continuïtat de l'activitat laboral, "*és convenient, si és possible, planificar les mesures que s'adoptaran per garantir la continuïtat durant l'absència*" i, si això no és possible, caldria que l'òrgan superior del treballador *"valori de forma motivada la necessitat de la intervenció per a la continuïtat del servei."*

En aplicació del principi de responsabilitat proactiva (art. 5.2 RGPD), el responsable, en aquest cas, l'Ajuntament, ha de respondre del compliment dels principis de protecció de dades, i per això, als efectes que interessen, no seria suficient al·legar una finalitat per a l'accés que en termes generals pot ser lícita, sinó que caldrà motivar-ho en base a les circumstàncies de cada cas.

En aquest cas, la consulta exposa que la documentació dipositada en l'equip local del treballador que es troba en situació de baixa, és essencial per poder seguir amb l'activitat que desenvolupa la Regidoria, i que no poder accedir a la informació de la Regidoria paralitza i afecta al desenvolupament de les accions que es fan a l'Ajuntament, de manera que, sempre segons la consulta, des de la baixa del treballador no s'ha pogut continuar amb l'activitat normal de la Regidoria.

Fer notar, en qualsevol cas que amb caràcter general caldria que l'Ajuntament valori els riscos que per a la informació de l'Ajuntament ha de tractar s'emmagatzemi de manera local en equips dels quals no n'existeix una còpia de seguretat. La garantia de la integritat i la disponibilitat d ela informació requeriria emmagatzemar la informació mitjançant sistemes que permetin fer-ne de manera periòdica còpies de seguretat periòdiques, que hauria de custodiar l'Ajuntament.

Tenint en compte tot l'exposat, i atesa la informació de què es disposa, en principi es podria considerar que el tractament objecte de consulta podria ser lícit per al compliment d'aquesta finalitat (garantir la continuïtat de la feina de la Regidoria en absència del treballador que es troba en situació de baixa), als efectes de la previsió de l'article 6.1,

apartat e) de l'RGPD, en connexió amb les previsions normatives a les que hem fet esment (normativa laboral i art. 87 LOPDGDD). Això, sempre que resulti necessari per assegurar el normal funcionament de la feina desenvolupada des de la Regidoria de l'Ajuntament -com sembla que seria el cas examinat, atesa la informació disponible-.

IV

Encara en relació amb la licitud de l'accés, la **pregunta C),** pregunta si es podria justificar l'accés a l'equip del treballador, per "*Corroborar si s'està incomplint les mesures de seguretat del Ajuntament, possibilitat que està comunicada i acceptada pels funcionaris".*

Sembla, per la informació disponible, que en aquest cas l'Ajuntament planteja si l'accés no ja en base a una finalitat de garantir la continuïtat de l'activitat de la Regidoria -qüestió ja comentada-, sinó per comprovar l'incompliment -per part del treballador- de les mesures de seguretat que, per la informació de què es disposa, l'Ajuntament podria haver previst en el protocol corresponent.

Cal recordar que, segons explica la consulta, en el cas plantejat el funcionari en qüestió "*té un afer disciplinari amb l'Ajuntament, encara pendent de resolució*."

Per la informació disponible, es desconeix si l'afer disciplinari referit per l'Ajuntament té cap vinculació amb un possible mal ús del treballador dels mitjans (equip informàtic, correu electrònic, etc), que l'Ajuntament hauria posat a la seva disposició, o si l'accés a l'equip, objecte de consulta, pot ser rellevant o necessari a aquests efectes, i en quina mesura.

A la vista de la informació disponible, aquest informe no pot determinar si els possibles indicis de mal ús o de "*possible incompliment de les mesures de seguretat*" per part del treballador, de què pugui disposar l'Ajuntament, serien suficients als efectes de justificar o considerar lícita o proporcionada la intervenció de l'equip del treballador en el cas concret que s'analitza.

Feta aquesta consideració, i en termes generals, convé recordar que, segons l'article 87.2 LOPDGDD, es considera lícit l'accés de l'empresari a continguts derivats de l'ús dels mitjans que facilita als seus treballadors, per a **"garantir la integritat d'aquests dispositius"**.

En la mesura, doncs, que la finalitat pretesa per l'Ajuntament, tingui per objectiu detectar possibles incompliments de les mesures de seguretat que aquest hagi prèviament posat en coneixement dels treballadors a través del protocol o de la formació que s'hauria donat als treballadors i, en definitiva, garantir l'ús adequat de l'equip posat a disposició del treballador i la integritat i seguretat de la informació i documentació que s'hi conté, en principi podria entendre's que l'accés respon a una finalitat prevista a la normativa que, per tant, pot ser lícita.

En aquest sentit, com ha fet avinent aquesta Autoritat en la Recomanació 1/2013, l'accés fonamentat en la finalitat de constatar un possible mal ús dels equips que l'Ajuntament posa a disposició dels treballadors), ha de ser proporcionat al tipus de risc que es pugui derivar del mal ús de l'equip o del compte de correu del treballador, en els termes que s'apunten en el punt 3 de l'apartat III de la Recomanació.

Per tant, per tal de considerar lícit l'accés a l'equip del treballador per corroborar el correcte compliment de les "mesures de seguretat" a què es refereix la consulta, caldria prèviament identificar aquest risc, i determinar si no hi ha mesures alternatives menys

intrusives per fer aquesta comprovació, tal i com es desprèn de la normativa i de la jurisprudència esmentades.

V

Pel que fa a la **pregunta E):** "*Que qualsevol actuació sigui escrupolosa amb la possibilitat de trobada de document de caràcter privat, tot i que estan prohibits temes personals en les eines de treball, vetllant i evitant en aquest cas, qualsevol obertura i accés en aquest continguts",* cal fer les següents consideracions.

La consulta fa referència a que els funcionaris de l'Ajuntament varen rebre formació en protecció de dades i que el protocol de seguretat de l'Ajuntament preveu, entre d'altres, que *"els recursos de l'entitat no poden utilitzar-se per finalitats privades".*

Als efectes de la normativa de protecció de dades, cal tenir en compte -com es desprèn de l'apartat III de la Recomanació 1/2013-, que encara que l'Ajuntament hagi determinat que els treballadors no poden fer ús dels equips, o del correu electrònic per motius personals o aliens a l'àmbit laboral (en el cas que ens ocupa, el protocol de l'Ajuntament determinaria que *"los recursos de la entidad no pueden utilizarse con fines privados"),* el treballador no sempre podrà evitar, per exemple, l'ús que facin terceres persones d'aquests correus, per remetre-li missatges de caràcter personal.

De la mateixa manera, si bé el protocol de l'Ajuntament, per la informació disponible, indica la prohibició de tenir documentació personal en els equips que l'empresa facilita als treballadors, no és descartable que l'accés a l'equip del treballador, que pot ser lícit en els termes apuntats, comporti l'accés a informació personal del propi treballador.

Des de la perspectiva dels principis de protecció de dades, es valora positivament la previsió que explicita la consulta, en el sentit que l'actuació de l'Ajuntament haurà de ser escrupolosa en cas que es trobi documentació de tipus privat, *"evitant en aquest cas qualsevol obertura i accés"* d'aquests continguts.

Sobre això, recordar que el principi de minimització (art. 5.1.c) RGPD) exigeix que les dades tractades han de ser les adequades, pertinents i limitades a allò necessari en relació amb les finalitats del tractament. En el cas que ens ocupa, ateses les finalitats esmentades (previstes en l'article 87 LOPDGDD, en connexió amb la normativa laboral estudiada), que poden habilitar l'accés i monitorització dels equips que l'empresa posa a disposició dels treballadors, no sembla proporcionat ni justificat, en principi, l'accés a informació privada, en els termes de la consulta.

Per tant, tal i com apunta la mateixa consulta, i en línia amb el que fa avinent aquesta Autoritat en la Recomanació 1/2013, vistes les finalitats de l'accés a l'equip del treballador segons es desprèn de la informació aportada, caldria articular la intervenció en l'equip del treballador, de manera que s'eviti l'accés a aquest contingut de tipus privat o aliè a la documentació de la Regidoria.

En aquest sentit responent a la **pregunta F** resulta convenient limitar l'accés a les persones que sigui estrictament necessari per a l'exercici de les seves funcions, fer la intervenció a partir d'una còpia o duplicat de la informació emmagatzemada, sense alterar la informació que consti a l'equip, i documentar tant la intervenció com les actuacions posteriors descrivint de manera detallada les actuacions realitzades i els resultats obtinguts.

Segons la Recomanació 1/2013, en aquest cas l'accés l'hauria de dur a terme la persona designada pel responsable de seguretat, en presència de la persona treballadora o, si això no és possible, del representant del personal i de la persona instructora o inspectora.

En relació amb aquesta qüestió, a la consulta s'indica "*Que l'accés seria fet per l'Administrador de sistemes extern –informàtic-".*

Tot i que es prevegi la intervenció d'un tècnic extern, l'accés a l'equip del treballador, i el tractament de la informació a la que s'accedeixi, haurà de produir-se seguint les indicacions de l'Ajuntament. En aquest cas en què l'accés es duu a terme per un tercer extern i aliè al responsable, correspondria a l'Ajuntament establir com s'ha de produir aquest accés a l'equip i el consegüent tractament de la informació, a través d'un contracte o acord d'encàrrec del tractament, en els termes previstos a l'article 28 RGPD, al que ens remetem.

Això, sens perjudici que, tant si l'accés es du a terme des de serveis propis de l'Ajuntament, com si s'articula a través d'un contracte d'encàrrec per tal que hi accedeixi un tercer aliè a l'Ajuntament (com ara una empresa externa), qualsevol tractament de dades personals es troba subjecte al necessari compliment del principi de confidencialitat (art. 5.1.f) RGPD), que obliga a qualsevol persona que accedeixi a les dades personals que puguin contenir-se en la documentació, arxius, o correu electrònic, si escau, de l'equip del treballador en qüestió.

És responsabilitat de l'Ajuntament, en qualsevol cas, informar a qualsevol de les persones designades per intervenir en l'accés a l'equip del treballador, dels seus deures i obligacions en matèria de seguretat, i en especial d'aquest deure de secret.

En aquest sentit, com fa avinent la Recomanació 1/2013, en aquest sentit pot ser recomanable fer signar a les persones que intervenen en aquestes operacions, un compromís de confidencialitat respecte de les dades a què puguin tenir accés.

VI

Pel que fa a la **pregunta G):** *"Si entenen que s'ha de comunicar aquesta acció al afectat, cas que considerin que es pot fer l'accés, tot i que la consulta es fa des de la perspectiva que el afectat no presta el seu consentiment.",* cal dir el següent:

Com es desprèn de l'article 87.3 *in fine* LOPDGDD, i com es posa de manifest no només en l'RGPD i la jurisprudència esmentada (STEDH Barbulescu i STC 61/2021, entre d'altres), sinó també en la Recomanació 1/2013, tenint en compte que la monitorització dels equips que l'empresari posa a disposició dels treballadors pot ser considerada una mesura intrusiva, cal assegurar que els treballadors, en aquest cas, el treballador que es troba de baixa, en tenen coneixement.

Com fa avinent la Recomanació 1/2013 (apartat III), l'accés als comptes de correu del treballador i, per extensió, podríem afegir, als equips que aquest empra per raons de feina, s'ha de dur a terme d'acord amb les normes d'ús que aprova l'empresa, *"que han d'advertir sobre els mecanismes de control de l'ús de les tecnologies que puguin afectar la privacitat de les persones, de les conseqüències que es poden derivar del control i les garanties per a les persones treballadores,* ***en especial el dret a ser-ne informat."***

Dit això, respecte en quin moment s'hauria d'informar el treballador atesa la finalitat que es persegueix, recordem que, segons s'exposa en l'apartat III de la Recomanació 1/2013, en el cas de l'accés per garantir la continuïtat de l'activitat de l'Ajuntament en absència,

en aquest cas per malaltia, del treballador, s'hauria de comunicar prèviament a aquest, i amb suficient antelació a la intervenció. Només si no fos possible aquesta comunicació prèvia, es podria informar el treballador posteriorment, al més aviat possible.

Pel que fa a l'accés amb finalitat de detectar un possible mal ús de l'equip per part del treballador, es considera que igualment la intervenció s'hauria de posar en coneixement previ del treballador afectat, llevat que l'Ajuntament consideri que això pot obstaculitzar les investigacions escaients.

Finalment, recordar que, per aplicació de les obligacions del responsable en matèria de protecció de dades (arts. 12, 13 i 14 RGPD), l'Ajuntament ha de facilitar informació als treballadors en relació amb la possibilitat d'exercir els seus drets d'accés, rectificació o supressió de les seves dades, entre d'altres (arts. 15 i ss. RGPD). Això, independentment de quina sigui la base jurídica del tractament (art. 6.1 RGPD).

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

Conclusions

L'accés a l'equip local del funcionari que es troba de baixa, amb la finalitat de garantir la continuïtat de l'activitat en absència del treballador i amb la finalitat de comprovar un possible mal ús de l'equip per part del treballador i protegir la integritat de la informació, es pot considerar lícit si resulta justificat per les circumstàncies concurrents.

Cal articular la intervenció en l'equip del treballador, de manera que s'eviti l'accés a contingut de tipus privat o aliè a la documentació de la Regidoria.

L'accés amb la finalitat de garantir la continuïtat de l'activitat en absència del treballador, se li ha de comunicar prèviament a la intervenció, llevat que no sigui possible. L'accés amb la finalitat de determinar un mal ús de l'equip, també s'ha de posar en coneixement del treballador, llevat que obstaculitzi les investigacions escaients. S'ha de fer en presència de la persona treballadora o, si això no és possible, del representant del personal.

L'accés s'ha de limitar a les persones que sigui estrictament necessari que han de quedar vinculades pel deure de confidencialitat. L'accés s'ha de fer a partir d'una còpia o duplicat de la informació emmagatzemada, sense alterar la informació que consti a l'equip, i documentar tant la intervenció com les actuacions posteriors descrivint de manera detallada les actuacions realitzades i els resultats obtinguts. Si intervé un tècnic extern, el tractament de la informació s'hauria de concretar en un contracte o acord d'encàrrec del tractament.

Barcelona, 29 de juliol de 2021