apdcat
Autoritat Catalana de Protecció de Dades

Dictamen en relació amb la consulta formulada per un ajuntament sobre la política d'ús dels sistemes d'informació i comunicació del consistori

Antecedents

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'un ajuntament, en què planteja diverses qüestions relacionades amb la política d'ús dels sistemes d'informació i comunicació que està elaborant el consistori.

En concret, en relació amb la regulació de l'accés i la gestió de les adreces personalitzades de correu electrònic corporatives, així com de les aplicacions corporatives, es formulen les qüestions següents:

> *"**A.** (...) En la baixa definitiva d'una adreça corporativa personalitzada de correu electrònic quan la persona usuària que té assignada la bústia deixa de prestar serveis a l'Ajuntament, tenim les consultes següents:*
>
> - *Cal elaborar un procediment intern que estableixi les normes d'ús dels sistemes d'informació en què s'informi del protocol de bloqueig de l'adreça corporativa personalitzada de correu electrònic i de com es gestionarà en cas de baixa definitiva i cal informar a les persones usuàries d'aquest procediment?*
> - *Cal crear un missatge de resposta automàtica previ al bloqueig de l'adreça corporativa personalitzada de correu electrònic que informi de la baixa de la persona usuària que té assignada l'adreça corporativa personalitzada i que indiqui una altra adreça de contacte per a la remissió de correus?*
> - *Es poden redireccionar de forma automàtica els correus electrònics entrants de l'adreça corporativa personalitzada de correu electrònic de la persona que deixa de prestar serveis a l'Ajuntament a una nova adreça?*
> - *L'Ajuntament pot recuperar, si és convenient, els missatges necessaris per a garantir el bon funcionament del servei amb caràcter previ a que la persona usuària deixi de prestar serveis a l'Ajuntament i en la seva presència? Si això no és possible, es poden recuperar els missatges i com s'ha de fer?*
> - *Es pot permetre a la persona usuària de l'adreça corporativa personalitzada que deixarà de prestar serveis a l'Ajuntament recuperar missatges personals abans que es bloquegi el compte de correu i que la persona ja no presti serveis.*
> - *Durant quant de temps s'ha de conservar el compte actiu de l'adreça corporativa personalitzada de correu electrònic de la persona usuària que ha deixat de prestar serveis per tal que no es pugui considerar com un període de temps poc raonable i desproporcionat?*
> - *Es pot deixar el compte inactiu de l'adreça corporativa personalitzada de correu electrònic a partir del dia següent a la data en què la persona usuària deixa de prestar serveis a l'Ajuntament?*

- *Es podria considerar adequat a la normativa de protecció de dades que l'adreça corporativa personalitzada de correu electrònic pugui estar activa durant el termini d'un mes i es faci constar un missatge de resposta automàtica en què es faci referència a que la persona ja no presta serveis a la corporació i que per a qualsevol tema es poden posar en contacte amb l'Ajuntament, fent constar el corresponent telèfon o adreça de correu electrònic.*
- *Una vegada passat el termini en què l'adreça corporativa personalitzada de correu electrònic pugui estar activa, s'ha d'eliminar o s'ha de conservar bloquejada i, si escau, durant quant de temps?*
- *A partir de la data en la qual deixa de prestar serveis la persona usuària, es podria descarregar el contingut de la bústia de correu electrònic i mantenir-ho bloquejat, a la vegada que es dona de baixa l'adreça corporativa personalitzada de correu electrònic? Si la resposta és afirmativa, durant quan de temps s'ha de conservar bloquejada aquesta informació?*

***B.** (...) Sobre l'accés a una adreça corporativa personalitzada de correu electrònic corporativa de persones usuàries del correu que es troben en situació de baixa temporal en la prestació de serveis, tenim les consultes següents:*

- *Quan una persona usuària del servei de correu està en situació de baixa temporal, en quines situacions i com l'Ajuntament pot accedir al contingut de la seva adreça corporativa personalitzada de correu electrònic?*

***C.** (...) Amb anterioritat a la situació de teletreball quan una persona usuària de les aplicacions estava de baixa no anava a treballar a les instal·lacions municipals i, per tant, no accedia a les aplicacions assignades des del seu ordinador de sobretaula. Amb el teletreball això ha canviat i les persones usuàries poden accedir estant de baixa a les aplicacions mitjançant els dispositius corporatius assignats o a través d'internet. Això fa que es puguin produir accessos indeguts durant aquesta situació de baixa i que calgui dur a terme un seguiment dels accessos realitzats per evitar possibles fuites d'informació i tenim les consultes següents:*

- *Quan una persona usuària de les aplicacions està en situació de baixa temporal en la prestació de serveis, en quines situacions i com pot l'Ajuntament monitoritzar un període de temps i accedir al registre d'accessos de les aplicacions a les quals la persona usuària està autoritzada a accedir?*

***D.** (...) Quan una persona usuària deixa de prestar serveis a l'Ajuntament pot sol·licitar còpia dels correus electrònics de la seva adreça personalitzada de correu electrònic corporatiu?"*

Analitzada la consulta i la documentació que l'acompanya, vista la normativa vigent aplicable, i d'acord amb l'informe de l'Assessoria Jurídica emeto el següent dictamen.

Fonaments Jurídics

I

(...)

II

La consulta planteja diverses qüestions relacionades amb la política d'ús dels sistemes d'informació i comunicació de l'Ajuntament, la qual es troba en fase d'elaboració.

Des del punt de vista de la protecció de dades és important tenir en compte que l'Ajuntament, com a responsable del tractament de la informació personal de què disposa (article 4.7) del Reglament (UE) 2016/679, del Parlament i del Consell Europeu, de 27 d'abril de 2016, General de Protecció de Dades (en endavant, RGPD)), li correspon la tasca de garantir i poder demostrar que els tractaments de dades que s'efectuen a través dels seus sistemes d'informació i dispositius que facilita al seu personal per a l'exercici de les seves funcions professionals s'adeqüen a la normativa de protecció de dades (article 5.2 RGPD, relatiu al principi de responsabilitat proactiva).

Això, en termes pràctics, requereix, entre d'altres actuacions (article 24 RGPD):

a) La realització d'una anàlisi de riscos.
b) La definició d'una política d'ús dels sistemes d'informació i dispositius digitals.
c) La implantació de mesures de seguretat tècniques i organitzatives apropiades al risc.

Aspectes que, cal dir, s'han de plantejar no només respecte les dades personals dels ciutadans de què disposa l'Ajuntament per a l'exercici de llurs competències, sinó també respecte les dades personals dels empleats municipals que empren els sistemes d'informació i altres eines corporatives per desenvolupar les tasques professionals que tenen encomanades.

Això obliga l'Ajuntament a tenir també en consideració les implicacions que, per a la privacitat i la protecció de dades d'aquests empleats municipals, pot comportar l'establiment de mesures de control sobre l'ús de les eines esmentades per part del consistori, en aplicació al marc normatiu vigent.

Sobre aquestes qüestions, cal fer esment a l'article 87 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (en endavant, LOPDGDD), que disposa el següent:

> *"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, l'Ajuntament-, del compliment per part de les persones treballadores de les seves obligacions laborals.

Especialment, l'article 52 del Text refós de la Llei de l'Estatut bàsic del treballador públic (TRLEBEP), aprovat pel Reial decret legislatiu 5/2015, de 30 d'octubre, 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 del Text refós de la Llei de l'Estatut dels Treballadors (ET), aprovat pel Reial decret legislatiu 2/2015, de 23 d'octubre, 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 (...)".*

Fer notar que la jurisprudència (a tall d'exemple, la STS de 26 de setembre de 2007 o la més recent STC 61/2021 a què ens remetem) ha admès que l'empresari pot establir controls sobre l'ús de les eines que posa a disposició de les persones treballadores per a la necessitat de coordinar i garantir la continuïtat de l'activitat laboral en els supòsits d'absències dels treballadors, per a la protecció dels sistemes d'informació, que poden ser afectats negativament per determinats usos, i per a la prevenció de les responsabilitats que per a l'empresari puguin derivar-se de formes il·lícites d'ús front a terceres persones.

Especialment rellevant és, en aquest sentit, la Sentència del Tribunal Europeu de Drets Humans (TEDH), cas *Barbulescu*, de 5 de setembre de 2017, en què el TEDH estableix determinats elements que caldria aplicar en aquest context. En síntesi, el TEDH fa referència a la informació que cal donar a les persones treballadores respecte les mesures que pot prendre l'empresari per 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 a les persones

treballadores, entre d'altres (apartat 210 de la STEDH de 5 de setembre de 2017, a què ens remetem).

Fer avinent també que aquesta Autoritat ha dictat la Recomanació 1/2013, sobre l'ús del correu electrònic en l'àmbit laboral (disponible al web de l'Autoritat), en què es fan diferents consideracions que resulten d'especial interès en el cas examinat, i a les que farem esment al llarg d'aquest dictamen.

III

Centrant-nos en les qüestions concretes plantejades en la consulta, bona part d'aquestes estan relacionades amb la regulació de l'accés i la gestió dels comptes de correu electrònic corporatives, amb adreça personalitzada, quan es dona de baixa l'adreça que té assignada una persona treballadora amb motiu de deixar de prestar serveis a l'Ajuntament de manera definitiva.

D'entrada, es planteja si "*cal elaborar un procediment intern que estableixi les normes d'ús dels sistemes d'informació en què s'informi del protocol de bloqueig de l'adreça corporativa personalitzada de correu electrònic i de com es gestionarà en cas de baixa definitiva"*, així com si "*cal informar les persones usuàries d'aquest procediment".*

Tal com es desprèn de l'article 87.3 de l'LOPDGDD, transcrit a l'apartat anterior, l'Ajuntament ha de comptar amb una política o manual que reculli els criteris o normes clares sobre les condicions d'ús dels sistemes d'informació i dispositius digitals que posa a disposició dels seus treballadors per desenvolupar llurs funcions professionals, les quals han d'advertir sobre els mecanismes de control sobre el seu ús que puguin afectar la privacitat de les persones treballadores, les conseqüències que es poden derivar d'aquest control i les garanties per a les persones treballadores, en especial el dret a ser-ne informades.

La prèvia informació a les persones treballadores sobre aquestes qüestions resulta cabdal per tal de poder considerar legítim el control per part de l'empresari respecte les eines esmentades i el seu ús (articles 5.1.a) i 6 RGPD), com ha recordat abastament la jurisprudència al respecte, com ara, entre d'altres, la STS de 26 de setembre de 2007 (FJ III):

> *"es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio. Por ello,* ***lo que debe hacer la empresa*** *de acuerdo con las exigencias de buena fe* ***es establecer previamente las reglas de uso de esos medios*** *–con aplicación de prohibiciones absolutas o parciales–* ***e***

> ***informar a los trabajadores de que va existir control y de los medios*** *que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinades conexiones. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado «una expectativa razonable de intimidad» en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo para la protección de los derechos humanos."*

Per la seva part, l'Esquema Nacional de Seguretat, aprovat pel Reial decret 311/2022, de 3 de maig, el qual resulta d'aplicació a l'Ajuntament de conformitat amb la disposició addicional primera de l'LOPDGDD, disposa, com a mesura de seguretat, l'establiment de normes d'ús del correu electrònic per al personal de l'organització (apartat 5.8).

Entre els diferents aspectes a tractar en aquestes normes o política d'ús, sens dubte seria convenient recollir les mesures que s'adoptaran per gestionar el compte personalitzat de correu electrònic corporatiu de les persones treballadores en cas de produir-se el cessament de la seva relació laboral amb l'Ajuntament.

Cal tenir present que, des del punt de vista de la protecció de dades, l'extinció de la relació laboral ha de comportar el cessament en el tractament de la informació personal de la persona treballadora per part de l'Ajuntament i, per tant, també de l'adreça del compte de correu electrònic personalitzat que se li hagi facilitat per al desenvolupament de les seves tasques professionals, en extingir-se alhora la finalitat que justificà el seu tractament (articles 5.1 b) i e) RGPD, principis de limitació de la finalitat i del termini de conservació, respectivament).

Això pot tenir implicacions tant per a la persona treballadora, qui podria tenir interès en disposar dels missatges privats o personals del seu compte corporatiu, com per al mateix Ajuntament, qui podria veure afectada la continuïtat de l'activitat municipal en major o menor mesura.

Apuntar que, tot i que es desconeix si en la política d'ús que s'està elaborant l'Ajuntament preveu admetre un cert ús privat dels comptes personalitzats de correu electrònic corporatius, cal tenir present, com apunta aquesta Autoritat a la Recomanació 1/2013, abans citada, que fins i tot respecte els comptes de correu dels quals s'estableixi un ús exclusivament professional la persona treballadora no sempre podrà evitar, per exemple, l'ús que facin terceres persones d'aquest correu, per remetre-li missatges de caràcter personal.

Als efectes de garantir un correcte tractament de la informació en aquests casos, és important disposar d'un procediment intern relatiu a l'ús del correu electrònic corporatiu que tingui en compte aquesta i altres circumstàncies, i on s'informi de manera prèvia al bloqueig del compte de la persona treballadora de la gestió que en farà l'Ajuntament i, per tant, de les mesures concretes que es poden adoptar en aquest sentit.

Recordar que la determinació i l'adopció d'aquestes mesures és, en tot cas, una decisió que correspon a l'Ajuntament, en atenció a les seves necessitats a l'hora de tractar la informació personal de què és responsable (articles 4.7 i 26 RGPD).

IV

En relació amb les possibles mesures a adoptar, en la consulta es planteja si *"cal crear un missatge de resposta automàtica previ al bloqueig de l'adreça corporativa personalitzada de correu electrònic que informi de la baixa de la persona usuària que té assignada l'adreça corporativa personalitzada i que indiqui una altra adreça de contacte per a la remissió de correus"* i si *"es poden redireccionar de forma automàtica els correus electrònics entrants de l'adreça corporativa personalitzada de correu electrònic de la persona que deixa de prestar serveis a l'Ajuntament a una nova adreça".*

En l'apartat III.4 de la Recomanació 1/2013, referit a l'accés al correu electrònic per part de l'empresa (en aquest cas, l'Ajuntament), s'identifiquen algunes actuacions que l'empresari pot dur a terme per gestionar correctament la informació amb motiu del cessament de la relació laboral de la persona treballadora.

En concret, s'apunta que en aquestes situacions cal comunicar-ho immediatament a la persona responsable de la gestió dels comptes de correu electrònic per tal que *"s'inutilitzin els codis d'usuari i les contrasenyes del treballador i, si escau, s'inclogui un missatge automàtic de resposta per al correu entrant que indiqui la nova adreça a la qual es poden adreçar els missatges per raons professionals."*

Per tant, en atenció a les necessitats concretes que puguin concórrer en el cas concret (per exemple, segons el lloc i/o càrrec de la persona treballadora i les funcions que ve desenvolupant), pot resultar una mesura adequada programar un missatge automàtic de resposta per a tots els correus entrants a la bústia de la persona treballadora que deixa de prestar serveis a l'Ajuntament, indicant que el compte en qüestió està en desús i la nova adreça de correu corporativa on es poden adreçar els correus per motius professionals.

Aquesta actuació és preferible al reenviament de forma automàtica dels correus electrònics entrants a una altra adreça de correu corporativa, atès que, en aquests casos, es produeix una manca de control sobre els correus electrònics en qüestió, per la qual cosa la informació privada que eventualment hi pogués constar podria acabar essent coneguda per persones no previstes per la persona remitent de la comunicació, podent contravenir no només la normativa de protecció de dades (article 5.1.e) RGPD, principi d'integritat i confidencialitat), sinó també altres drets constitucionalment protegits (intimitat i secret de les comunicacions (article 18.1 i 3 CE)).

V

En la consulta també es planteja si *"l'Ajuntament pot recuperar, si és convenient, els missatges necessaris per a garantir el bon funcionament del servei amb caràcter previ a*

que la persona usuària deixi de prestar serveis a l'Ajuntament i en la seva presència" i si això no és possible *"si es poden recuperar els missatges i com s'ha de fer".*

Tal com indica aquesta Autoritat a la Recomanació 1/2013, un dels objectius que podria justificar l'accés al correu electrònic corporatiu de les persones treballadores per part de l'empresari, en aquest cas l'Ajuntament, i sempre que se n'hagi informat adequadament, és el de garantir la continuïtat de l'activitat normal de l'empresa, atès que aquesta podria veure's afectada en cas de no disposar de certa informació professional (article 87 LOPDGDD, en connexió amb la normativa laboral i la jurisprudència existent).

També en aquest cas, com s'assenyala en la dita Recomanació, és convenient planificar i definir en la política d'ús dels sistemes d'informació -i informar-ne els treballadors- les mesures que s'adoptaran en aquest sentit en cas d'absència de les persones treballadores i també en el cas de cessament de la relació laboral (apartat III. 2 i 4).

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

Així, en el cas de cessament de la relació laboral, i seguint les consideracions formulades a la Recomanació 1/2013, així com en la Recomanació CM/REC (2015) 5, d'1 d'abril de 2015, del Comitè de Ministres del Consell d'Europa, relativa al tractament de dades personals en el context de la relació de treball, podria establir-se en la política d'ús que l'accés al compte de correu electrònic corporatiu de les persones treballadores que pogués justificar-se en aquesta finalitat de garantir la continuïtat de l'activitat normal de l'Ajuntament té per finalitat recuperar la informació vinculada estrictament a l'activitat professional de la persona treballadora que causa baixa definitiva a l'Ajuntament quan aquesta resulta essencial per continuar amb l'activitat normal municipal; que l'accés es durà a terme, sempre que sigui possible, amb anterioritat al dia en què se cessa efectivament la relació laboral amb l'Ajuntament, davant la presència de la persona treballadora i, si escau, d'un tercer; que, quan això no sigui possible, l'òrgan superior de la persona ex treballadora haurà de valorar de forma motivada la necessitat de la intervenció i haurà d'identificar la informació concreta a la que cal accedir, i que l'accés es comunicarà, si és possible, a la persona ex treballadora; i que, en cap cas, l'accés abastarà missatges que es puguin identificar clarament com a privats o personals, o bé aquells que la mateixa persona treballadora assenyali d'aquesta naturalesa.

Cal tenir present que, ateses les finalitats previstes en l'article 87 de l'LOPDGDD, en connexió amb la normativa laboral examinada, que poden habilitar l'accés i monitorització dels equips que l'empresa posa a disposició dels seus treballadors, l'accés a informació privada no resultaria ni proporcionat ni justificat.

VI

En la consulta també es planteja si *"es pot permetre a la persona usuària de l'adreça corporativa personalitzada que deixarà de prestar serveis a l'Ajuntament recuperar*

missatges personals abans que es bloquegi el compte de correu i que la persona ja no presti serveis."

Tal com es fa avinent en la Recomanació 1/2013 (aparat II.4), és important establir a la política d'ús un termini màxim de conservació dels missatges privats, acomplert el qual s'han d'esborrar, així com fomentar la creació de carpetes per emmagatzemar correus d'aquesta naturalesa que en permetin la identificació fàcilment en cas d'un eventual accés per part de l'empresari al compte de correu corporatiu.

També es fa avinent en la dita Recomanació (apartat III.4) que, donat el cas de cessament de la relació laboral, l'empresa (l'Ajuntament) ha de facilitar a la persona treballadora l'obtenció dels missatges privats del dit compte de correu corporatiu, sempre que no superin el període màxim de conservació que s'hagi establert a la política d'ús. I que, en aquest cas, l'accés s'ha de produir en presència de la persona treballadora per tal d'identificar els missatges de caràcter exclusivament personal, qui podria decidir esborrar aquests missatges privats o bé transferir-los a un altre compte de correu.

VII

En la consulta es plantegen també algunes qüestions relacionades amb el fet de mantenir activa durant un cert temps l'adreça personalitzada de correu electrònic corporativa de la persona treballadora que deixa de prestar serveis a l'Ajuntament. En concret:

- *"Durant quant de temps s'ha de conservar el compte actiu de l'adreça corporativa personalitzada de correu electrònic de la persona usuària que ha deixat de prestar serveis per tal que no es pugui considerar com un període de temps poc raonable i desproporcionat."*
- *"Es pot deixar el compte inactiu de l'adreça corporativa personalitzada de correu electrònic a partir del dia següent a la data en què la persona usuària deixa de prestar serveis a l'Ajuntament"*
- *"Es podria considerar adequat a la normativa de protecció de dades que l'adreça corporativa personalitzada de correu electrònic pugui estar activa durant el termini d'un mes i es faci constar un missatge de resposta automàtica en què es faci referència a que la persona ja no presta serveis a la corporació i que per a qualsevol tema es poden posar en contacte amb l'Ajuntament, fent constar el corresponent telèfon o adreça de correu electrònic."*
- *"Una vegada passat el termini en què l'adreça corporativa personalitzada de correu electrònic pugui estar activa, s'ha d'eliminar o s'ha de conservar bloquejada i, si escau, durant quant de temps."*

Com s'ha avançat a l'apartat III d'aquest dictamen, des del punt de vista de la protecció de dades, l'extinció de la relació laboral ha de comportar el cessament en el tractament de la informació personal de la persona treballadora per part de l'Ajuntament i, per tant, també del seu compte de correu electrònic corporatiu, en extingir-se la finalitat que justifica el seu tractament.

Aquesta és una exigència que deriva del principi de limitació de la finalitat (article 5.1.b) RGPD), segons el qual *"los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con*

dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales".

Principi que s'ha de posar en consonància amb el principi de limitació del termini de conservació (article 5.1.e) RGPD), segons el qual *"los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado".*

Sobre això, segons el considerant 39 de l'RGPD: "(…) *Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. (…)."*

A banda d'aquests principis, resulta especialment rellevant el dret de supressió regulat a l'article 17 de l'RGPD, d'acord amb el qual:

> *"1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:*
> *a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;*
> *b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;*
> *c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;*
> *d) los datos personales hayan sido tratados ilícitamente;*
> *e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;*
> *f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.*
> *(...)."*

Es desprèn d'això que el responsable del tractament (article 4.7 RGPD) ha de conservar les dades personals durant el menor temps possible i que, en la determinació d'aquest termini de conservació, ha de tenir-se en compte la finalitat per a la qual es necessita el tractament de les dades, de tal manera que, un cop assolida la finalitat, les dades

personals hauran d'ésser suprimides. També caldria tenir en compte les obligacions de conservació de les dades durant un temps determinat que puguin establir disposicions aplicables, de tal manera que, acomplerts aquests terminis, és quan les dades personals hauran de suprimir-se.

Tal i com disposa la mateixa normativa de protecció de dades, la supressió, quan és pertinent, no equival necessàriament a l'esborrat o la destrucció de la informació personal, sinó al seu bloqueig.

En concret, l'article 32 de l'LOPDGDD estableix el següent:

> *"1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.*
> *2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos.*
> *3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.*
> *4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.*
> *(...)."*

Així doncs, les dades personals s'han de suprimir un cop deixen de ser necessàries o pertinents per a la finalitat per a la qual es van recollir o, si escau, un cop finalitzats els terminis de conservació establerts per la llei, fet que comportarà el seu bloqueig durant els terminis de prescripció en què es pugui exigir algun tipus de responsabilitat derivada del tractament. Acomplert aquest termini, el qual pot variar en funció de la informació tractada i de les responsabilitats que es poden generar, s'ha de procedir a l'eliminació efectiva de la informació personal.

Això traslladat al cas que ens ocupa, i donant així resposta a les preguntes formulades, implica que, amb caràcter general, la supressió (i, per tant, bloqueig) de l'adreça personalitzada de correu electrònic corporatiu de la persona treballadora que deixa de prestar serveis a l'Ajuntament s'hauria d'efectuar en el moment en què es produeix l'extinció de la relació laboral (podria ser el dia següent a la data en què deixa de prestar serveis).

Ara bé, amb la finalitat, quan escaigui, de garantir la continuïtat del servei, pot resultar admissible mantenir "activa" l'adreça corporativa en qüestió, malgrat que la persona titular ja no presti serveis a l'Ajuntament, durant un cert temps. Fer notar que no tots els llocs de

treball podrien justificar que es mantingués l'adreça operativa, dependrà del càrrec o de les funcions que tenia assignades la persona ex treballadora.

Cal tenir present que, en tot cas, aquesta actuació hauria de limitar-se a la programació del missatge de resposta automàtica a què s'ha fet esment en l'apartat IV d'aquest dictamen, en què s'informa als remitents dels correus entrants que el compte en qüestió està en desús i l'adreça a què s'han d'adreçar els missatges en cas de voler contactar amb el departament o àrea municipal corresponent.

Respecte el temps en què podria mantenir-se amb aquest objectiu activa l'adreça de correu electrònic, fer notar que no hi ha una previsió normativa en aquest sentit, si bé, en aplicació del principi de limitació de la conservació de les dades (article 5.1.e) RGPD), no hauria d'allargar-se més enllà del temps estrictament necessari per assolir la finalitat de no perdre informació rellevant per a l'Ajuntament.

Com a orientació, assenyalar que l'Autoritat Belga de Protecció de Dades recomana un termini d'un mes amb caràcter general, que podria, en atenció al context i les funcions o càrrec que ostentava la persona ex treballadora, ampliar-se fins un màxim de tres mesos (Decisió emesa el 29 de setembre de 2020, disponible al seu web).

Vist això, l'opció plantejada a la consulta consistent en mantenir activa l'adreça durant el termini d'un mes i fent-hi constar un missatge de resposta automàtica informant sobre la nova adreça o telèfon de contacte de la persona a qui adreçar-se resultaria adequada a la normativa de protecció de dades.

Durant aquest termini en què estigui en funcionament el missatge de resposta automàtica, la bústia de correu electrònic hauria de mantenir-se bloquejada de tal manera que no es pugui accedir al seu contingut.

A tot això, la consulta planteja si *"a partir de la data en la qual deixa de prestar serveis la persona usuària, es podria descarregar el contingut de la bústia de correu electrònic i mantenir-ho bloquejat, a la vegada que es dona de baixa l'adreça corporativa personalitzada de correu electrònic"* i, en cas afirmatiu, *"durant quan de temps s'ha de conservar bloquejada aquesta informació."*

La normativa de protecció de dades obliga el responsable del tractament (l'Ajuntament) a bloquejar les dades quan en dugui a terme la supressió (article 32.1 LOPDGDD).

En un cas com el plantejat, en què cal donar de baixa l'adreça personalitzada de correu electrònic corporatiu amb motiu del cessament de la relació laboral de la persona treballadora, respecte el contingut de la bústia (el conjunt de missatges que s'hi poden contenir), per tal de poder complir amb aquesta obligació de bloqueig, seria raonable que a tal efecte aquesta informació pogués ésser descarregada o guardada pel responsable i conservar-la degudament bloquejada.

Tenint en compte que es tracta d'una eina facilitada per al desenvolupament de les tasques professionals de les persones treballadores i vistes les pautes i recomanacions que aquestes persones han de seguir quan s'admet un ús privatiu d'aquesta eina (configuració dels missatges, organització en carpetes, respectar el període de conservació fixat, verificar periòdicament els que s'han d'eliminar, possibilitat de

recuperar els missatges abans del cessament de la relació laboral, etc.), a priori en la bústia de correu electrònic corporatiu no hi haurien de constar missatges de naturalesa privada o personal de la persona ara ex treballadora, si bé tampoc és possible descartar-ho amb tota seguretat. El mateix podria ocórrer malgrat que el compte de correu corporatiu es facilités per a motius exclusivament professionals.

Per això, com a garantia addicional per al respecte als drets de la persona ex treballadora, seria convenient que abans de descarregar el contingut de la bústia es dugués a terme una revisió d'aquesta per tal de detectar correus que, en atenció a l'assumpte, indueixin a pensar que es tracta de missatges de caràcter privat o personals, o bé per localitzar carpetes d'emmagatzematge de correus que puguin haver-se identificat com a privades o personals, i esborrar-ho (sense accedir al seu contingut).

Fet això, i un cop descarregada la informació, s'ha de conservar degudament bloquejada i no es podrà tractar per a cap finalitat, tret per a la posada a disposició de les dades als jutges i tribunals, al Ministeri Fiscal o a les administracions públiques competents, en particular de les autoritats de protecció de dades, per a l'exigència de possibles responsabilitats derivades del tractament (article 32.3 LOPDGDD).

El termini durant el qual s'ha de mantenir la informació bloquejada pot variar en funció de la seva naturalesa i de les responsabilitats que es poden generar i, un cop acomplert, s'haurà de procedir a l'eliminació efectiva d'aquesta informació (article 32.2 LOPDGDD).

VIII

La consulta també planteja *"quan una persona usuària del servei de correu està en situació de baixa temporal, en quines situacions i com l'Ajuntament pot accedir al contingut de la seva adreça corporativa personalitzada de correu electrònic."*

Tal com es posa de manifest a l'apartat III.2 de la Recomanació 1/2013, l'absència d'un treballador, especialment si és de llarga durada, pot comportar problemes per a la continuïtat de l'activitat normal de l'empresa, si no es pot accedir a un determinat compte de correu.

L'Autoritat posa l'èmfasi en la necessitat de planificar -i deixar constància en la política d'ús- les mesures que s'adoptaran per garantir la continuïtat durant l'absència d'aquesta persona, de tal manera que no sigui necessari l'accés de l'empresari al seu compte de correu pel risc que això pot comportar per als drets de la persona treballadora.

Entre aquestes mesures, pot preveure's, a tall d'exemple, que la persona treballadora pot eliminar o traslladar a una carpeta personal tots els missatges privats o de caire personal, i autoritzar l'accés a un altre treballador, adoptant els canvis pertinents, tant a l'inici com a la fi del període en què causi baixa, pel que fa al canvi de les contrasenyes; i/o transferir la informació necessària per continuar amb l'activitat durant la seva absència.

Si això no és possible, per exemple en cas d'absència imprevista de la persona treballadora, és necessari que l'òrgan superior de la persona treballadora absent valori de forma motivada la necessitat de la intervenció per a la continuïtat del servei (necessitat improrrogable lligada a l'activitat laboral).

També cal comunicar aquest accés a la persona treballadora amb antelació, si és possible, o bé amb caràcter posterior quan no hagi estat possible (tan aviat com sigui possible).

Aquest accés s'ha de realitzar en presència o sota la supervisió de l'òrgan superior de la persona treballadora i, en cas que se li hagi pogut comunicar, amb la seva assistència o de la persona que designi la persona interessada, si ho desitja.

No es pot accedir en cap cas, per aquest motiu, als missatges que la persona treballadora hagi assenyalat com a privats o que tingui emmagatzemats en una carpeta identificada com a privada o personal.

IX

Per altra banda, en la consulta es posa de manifest que, amb anterioritat a la situació de teletreball, quan una persona usuària de les aplicacions corporatives estava de baixa no anava a treballar a les instal·lacions municipals i, per tant, no accedia a les aplicacions assignades des del seu ordinador de sobretaula, però que això, amb el teletreball, ha canviat i les persones usuàries poden accedir-hi estant de baixa mitjançant els dispositius corporatius assignats o a través d'internet.

Això, sosté, fa que es puguin produir accessos indeguts durant aquesta situació de baixa i que calgui dur a terme un seguiment dels accessos realitzats per evitar possibles fuites d'informació.

Vist això, planteja *"quan una persona usuària de les aplicacions està en situació de baixa temporal en la prestació de serveis, en quines situacions i com pot l'Ajuntament monitoritzar un període de temps i accedir al registre d'accessos de les aplicacions a les quals la persona usuària està autoritzada a accedir."*

Recordar que correspon a l'Ajuntament, com a responsable, establir en la política d'ús que està elaborant els criteris generals i les normes que escaiguin per a l'adequada utilització, no només del correu electrònic corporatiu, sinó també dels seus sistemes d'informació, els quals posa a disposició dels seus treballadors per a que aquests actuïn amb responsabilitat i estiguin informats del control que pot exercir l'Ajuntament en l'ús d'aquests sistemes.

Tenint en compte que l'Ajuntament ha de ser capaç de demostrar que el tractament de dades a través dels seus sistemes d'informació s'adequa a la normativa de protecció de dades (article 5.2 RGPD), cal reconèixer-li la possibilitat de poder dur a terme, a través de les persones designades per aquesta funció, les tasques de control i seguiment que siguin necessàries en les infraestructures comunes i en les estacions de treball assignades al seu personal a l'efecte de comprovar i verificar que l'ús dels sistemes d'informació i aplicacions corporatives s'ajusta al que estableix la política d'ús i no genera incidents de seguretat.

Fer notar que aquesta mena de control ha de ser proporcionat al tipus de risc que es pugui derivar del mal ús dels sistemes d'informació per a l'Ajuntament o terceres

persones per part de totes aquelles persones que tenen autoritzat l'accés als sistemes d'informació (no hauria de ser una mesura pensada només per als treballadors que es troben prestant serveis en la modalitat de teletreball i que es troben absents amb motiu d'una baixa per malaltia o d'altra índole).

Vist això, l'Ajuntament podria establir en la política d'ús les limitacions en l'ús del correu electrònic i en els altres sistemes d'informació que calgui introduir durant el període en què s'estigui de baixa, que, amb la finalitat de garantir el bon funcionament dels sistemes d'informació i de fer un seguiment de la seva adequada utilització per part del seu personal, disposa d'eines i mitjans de control per supervisar i fer aquest seguiment, els quals, per exemple, permeten registrar l'accés als sistemes d'informació per part dels seus usuaris (identificació de l'usuari, dia, hora, recurs a què s'accedeix i motiu de l'accés), i el període de temps en què es revisarà la informació de control registrada (per exemple, un cop al mes).

Seria convenient també de les possibles conseqüències en el cas de l'existència d'indicis d'un mal ús dels sistemes d'informació per part dels treballadors, per incomplir les normes.

X

Finalment, a la consulta es planteja si *"quan una persona usuària deixa de prestar serveis a l'Ajuntament pot sol·licitar còpia dels correus electrònics de la seva adreça personalitzada de correu electrònic corporatiu."*

Respecte els correus de naturalesa privada o personal, com s'ha vist, caldria facilitar-ne l'accés de la persona treballadora abans de la seva marxa definitiva del lloc de treball, per bé que, davant d'una petició posterior d'accés a aquesta informació, no hi hauria d'haver, a priori, inconvenients des del punt de vista de la protecció de dades, atès que es tractaria d'informació a què podria tenir accés en exercici del seu dret d'accés a la informació que li és pròpia, en els termes de l'article 15 de l'RGPD.

Respecte els correus professionals, l'article 15 de l'RGPD permetria donar accés a les dades directament vinculades a la persona treballadora (o millor a la seva condició de persona remitent o receptora del missatge) però en canvi no sembla que pugui abastar l'accés a informació de terceres persones que pugui constar en els dits correus.

Respecte aquesta informació cal tenir present que es tractaria d'informació que figuraria en poder de l'Ajuntament com a conseqüència de l'exercici de les funcions encomanades a la persona que en demana l'accés. Per tant, es tractaria d'informació pública als efectes de l'article 2.b) de la Llei 19/2014, del 29 de desembre, de transparència, accés a la informació pública i bon govern (en endavant, LTC), i, conseqüentment, sotmesa al règim del dret d'accés (article 18 LTC).

L'article 18 de l'LTC reconeix el dret de les persones a *"accedir a la informació pública, a què fa referència l'article 2.b, a títol individual o en nom i representació de qualsevol persona jurídica legalment constituïda*" (apartat 1).

Ara bé, cal tenir en compte que aquest dret d'accés no és absolut i pot ser denegat o restringit per les causes expressament establertes a les lleis. Als efectes que interessen, cal tenir present que en els correus professionals sol·licitats constarà informació pròpia de la persona ex treballadora, a què podria tenir accés sobre la base de l'article 15 de l'RGPD, però també i principalment informació de terceres persones. Això, obligaria a tenir present les limitacions i criteris previstos a la legislació de transparència (articles 23 i 24 LTC), i els principis de la normativa de protecció de dades personals.

Fer notar, en aquest punt, que aquesta Autoritat ha tingut l'oportunitat d'examinar l'eventual accés i obtenció de còpia dels correus professionals per part d'una persona ex treballadora d'un ens local en l'informe IAI 2/2021, disponible en el web de l'Autoritat.

Tal com es fa avinent en aquest informe, en atenció a les funcions que tingués atribuïdes la persona ex treballadora, ens podríem trobar davant d'informació que podria ser de diversa naturalesa i afectar en major o menor grau la privacitat de les persones a què fa referència.

D'entrada, l'accés de la persona sol·licitant i l'obtenció d'una còpia dels correus professionals en què es continguin dades personals especialment protegides de terceres persones, un cop finalitzada la seva relació laboral amb l'Ajuntament, hauria de veure's en tot cas limitat sobre la base del que preveuen els articles 23 de l'LTC i 15.1 de la *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno* (LTC)).

Però més enllà d'això, en el contingut d'aquests correus professionals també hi podrien constar dades mereixedores d'una especial reserva o confidencialitat en atenció a la concurrència de determinades circumstàncies qualificades (per exemple, situacions de vulnerabilitat social, dades de menors, dades relacionades amb la violència de gènere, etc.) o en atenció a la naturalesa dels assumptes tractats per la persona ex treballadora segons les seves tasques o funcions assignades (membres de la policia local, personal de l'àrea de serveis socials, etc.).

També caldria tenir present que l'accés pretès podria afectar un gran volum de persones. Si bé el nombre d'afectats no és pròpiament un criteri decisiu a l'hora de poder limitar l'accés s'ha de tenir en compte que quan les persones afectades són molt nombroses això pot comportar una sèrie de problemes per poder atendre la sol·licitud d'accés amb les degudes garanties, en concret, atorgar el tràmit d'audiència que preveu l'article 31 de l'LTC i valorar, cas per cas, si ha de prevaler la protecció de dades personals o el dret d'accés de la persona reclamant.

Una ponderació raonada entre els diferents drets i interessos en joc que caldria fer d'acord amb l'article 24.2 de l'LTC, obligaria a tenir en compte aquesta circumstància que pot comportar una denegació de l'accés a aquesta informació en cas de no quedar suficientment acreditada la rellevància que pugui tenir per a la persona sol·licitant disposar d'aquesta informació.

Si bé no és obligatori incloure a la sol·licitud els motius pels quals es demana l'accés (articles 18.2 i 26.2 LTC), de no fer-ho, aquest element no es pot tenir en compte a l'hora de valorar els diferents drets i interessos en joc. Així, si no s'addueix cap motiu concret,

l'accés caldria entendre'l emmarcat dins la finalitat de la pròpia llei de transparència (article 1.2 LTC).

Per tot això, amb caràcter general, no apareixeria com a justificat, des del punt de vista de la protecció de dades, l'obtenció de manera generalitzada per una persona ex treballadora d'una còpia del conjunt de correus electrònics professionals. Això, sens perjudici que en algun cas concret pogués resultar justificat l'accés i l'obtenció de còpia de determinats correus electrònics en atenció a les circumstàncies o motius concrets que pogués al·legar (per exemple, en cas de tractar-se d'informació necessària per al seu dret de defensa).

A tot això, destacar que l'LTC no estableix cap termini pel que fa a la conservació de la informació i documentació pública, als efectes de garantir l'exercici del dret d'accés (article 18 LTC). Per tant, no és obligatori conservar la informació de què es disposa per atendre eventuals peticions d'accés, més enllà dels terminis de conservació previstos en les disposicions que resultin d'aplicació al cas concret.

En aquest cas, com s'ha vist, el cessament de la relació laboral ha de comportar la supressió del compte de correu electrònic corporatiu de la persona treballadora, la qual cosa ha de donar lloc al seu bloqueig, en els termes de l'article 32 de l'LOPDGDD i amb les particularitats assenyalades al fonament jurídic VII.

Tal com ha posat de manifest aquesta Autoritat a l'informe IAI 6/2022 (disponible al web), el bloqueig d'informació personal no hauria de buidar de contingut la possibilitat d'exercir altres drets, com ara, el dret d'accés a informació pública, en els termes de la legislació de transparència.

La comunicació de dades bloquejades en aquest cas tindria per finalitat complir amb una obligació del responsable, fonamentada en la Constitució (art. 105.b) CE) i en l'LTC, per la qual cosa, com es va posar de manifest al dictamen CNS 76/2016 (disponible al web), podria resultar lícita sobre la base jurídica de l'article 6.1.c) de l'RGPD.

Acomplert el termini de bloqueig de la informació que escaigui, s'haurà de procedir a l'eliminació efectiva dels correus electrònics.

Per tant, fer notar que l'atenció d'un eventual dret d'accés (i obtenció de còpia) d'una persona ex treballadora en relació amb els correus electrònics es pot de dur a terme mentre l'Ajuntament disposi d'aquesta informació pública.

Conclusions

La política d'ús dels sistemes d'informació i dispositius digitals que està elaborant l'Ajuntament ha d'abastar normes clares sobre la gestió que es farà del compte de correu electrònic corporatiu personalitzat, i sobre els accessos a la informació que conté, tant amb motiu de cessament de la relació laboral com en cas d'absència temporal de la persona treballadora, tenint en compte les consideracions fetes als apartats III a VIII d'aquest dictamen.

També ha d'incloure previsions específiques respecte l'ús adequat dels sistemes d'informació per part del seu personal i el control que en pot fer l'Ajuntament per garantir-ne la seguretat i el bon funcionament.

Respecte les peticions d'accés i obtenció de còpia dels correus electrònics per part de persones ex treballadores, cal tenir en compte les observacions fetes a l'apartat X d'aquest dictamen.

Barcelona, 12 de desembre 2022