Autoritat Catalana de Protecció de Dades

Dictamen en relació amb la consulta formulada per un Ajuntament en relació amb la consideració del correu electrònic corporatiu com a dada personal i les conseqüències del seu ús per al remitent

Es presenta davant l'Autoritat Catalana de Protecció de Dades una consulta formulada per un Ajuntament, en què es demana un dictamen a aquesta Autoritat en relació amb la consideració del correu electrònic corporatiu com a dada personal, i les conseqüències que el seu ús pot tenir per al remitent, en diverses situacions.

Analitzada la consulta, que s'acompanya d'informe de la Secretaria General de l'Ajuntament sobre la qüestió plantejada, vista la normativa vigent aplicable, i d'acord amb l'informe de l'Assessoria Jurídica es dictamina el següent:

I

(...)

II

La consulta pregunta, d'entrada, si el correu corporatiu format pel primer cognom, inicial del segon cognom i inicial del nom, així com la identificació de la corporació a la que pertany, es considera dada personal, protegida per la normativa de protecció de dades.

Així mateix, la consulta pregunta el següent:

> *"L'enviament d'un correu electrònic per un membre de la corporació a un altre membre o membres de la corporació, tractant temes sobre la mateixa, i posant en còpia una adreça de correu de fora de la corporació, seria susceptible d'incórrer en vulneració de la normativa sobre protecció de dades? Quines conseqüències o accions es poden interposar en aquest supòsit, enfront la persona que forma part de la corporació i titular del compte de correu corporatiu, que ha fet l'enviament (remitent) al correu d'altres membres de la corporació, posant en còpia una adreça de correu electrònic de fora de la corporació? Ha incorregut el remitent en alguna infracció de la normativa sobre protecció de dades?*
>
> *La mateixa situació, però en el cas que l'enviament es fes, per un membre de la corporació, però des de la seva adreça de correu personal, podria incorre en vulneració de la normativa sobre protecció de dades? quines conseqüències o accions es podrien interposar enfront dita persona?"*
>
> La consulta afegeix que, en tots dos casos, l'enviament sobre el que es pregunta és sempre *"sense el consentiment del destinatari o destinataris del correu membres de la corporació de facilitar la seva adreça de correu electrònic a un tercer, no membre de la corporació".*

Situada la consulta en aquests termes, cal partir de la base que, segons l'article 4.1) del Reglament (UE) 2016/679, de 27 d'abril, general de protecció de dades (RGPD), són dades de caràcter personal *"toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;".*

Per tant, d'entrada, qualsevol informació que permeti identificar directa o indirectament una persona física és dada personal, i queda protegida pels principis i garanties de la normativa de protecció de dades (RGPD i Llei orgànica 3/2018, de 5 de desembre, de Protecció de dades personals i garantia dels drets digitals (LOPDGDD)).

Segons el considerant 26 de l'RGPD: *"(...). Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. (...)."*

Als efectes d'aquest dictamen resulten d'especial interès la Recomanació 1/2013 de l'Autoritat Catalana de Protecció de Dades, sobre l'ús del correu electrònic en l'àmbit laboral, així com el *"Manual de bon ús del correu electrònic. Guia per a les persones treballadores per a la protecció de la privacitat en l'ús del correu electrònic",* disponibles al web de l'Autoritat (www.apdcat.cat).

Segons la Recomanació esmentada (apartat 2), una adreça de correu electrònic es pot definir com *"el conjunt de paraules o signes que identifiquen l'emissor o el receptor d'un missatge de correu electrònic. S'elabora a partir d'un conjunt de paraules o signes lliurement escollits, normalment, pel seu titular o per la organització a la qual pertany, amb l'únic límit que aquesta adreça no coincideixi amb la d'una altra persona. Està formada per una identificació de l'usuari, seguida del signe @ i, a continuació, el domini (identificació facilitada pel proveïdor del servei de correu, amb un punt, i unes sigles que poden identificar l'activitat de l'organització (p. ex. ".org") o les sigles del país (p. ex. ".es" o ".cat").*

Tal i com exposa la Recomanació, podem distingir diferents tipus d'adreces:

- Adreces personalitzades: adreces que contenen directament informació sobre el seu titular. Habitualment, en les adreces personalitzades es pot utilitzar el nom i cognoms complet, només les inicials, o la inicial del nom i el cognom, etc. Aquestes adreces de correu electrònic identifiquen directament el titular del compte i per tant s'ha de considerar com a dada de caràcter personal.

- Adreces no personalitzades: són aquelles que, tot i que es tracta d'una adreça vinculada a un compte de correu d'una persona física determinada, no contenen informació sobre el seu titular (empren una combinació alfanumèrica abstracta o sense cap significat). En aquest cas, l'adreça per si sola no identificaria la persona que n'és titular. Però aquesta persona pot ser fàcilment identificable, sense un esforç desproporcionat, bé perquè l'adreça pot aparèixer juntament amb altres dades que en permeten la identificació, bé pel contingut del missatge, bé a través de les dades de què disposa el servidor de correu. Per tant, aquesta adreça també seria dada de caràcter personal.

- Adreces de correu electrònic genèriques: són les que responen a un compte genèric, d'ús compartit o d'una àrea de l'organització (per exemple, consultes@empresa.cat). En aquest cas, l'adreça de correu electrònic no es pot vincular a una persona física identificada o identificable, sinó que la poden atendre habitualment usuaris diferents. Per tant, no es pot considerar dada de caràcter personal.

En línia amb això, com ha fet avinent aquesta Autoritat en diversos informes (CNS 55/2019, IAI 18/2019, IAI 2/2021, o CNS 36/2022, que es poden consultar al web de l'Ajuntament), les adreces de correu electrònic laborals o professionals que es poden associar a persones físiques identificables (art. 4.1 RGPD), s'han de considerar com a dada de caràcter personal.

Com es fa avinent en el Dictamen CNS 4/2011 *"Cal tenir en compte que una adreça de correu electrònic apareixerà sempre necessàriament vinculada a un domini concret, de tal manera que és possible procedir a la identificació del seu titular mitjançant la consulta del servidor en què es gestioni aquest domini, sense que això requereixi un esforç desproporcionat per part de qui procedeix a la identificació. D'altra banda, les adreces de correu electrònic dels treballadors d'una empresa (pública, en aquest cas) normalment es configuren de tal manera (nom_cognom@nom del domini) que fàcilment permeten identificar als seus titulars. Per tant, d'acord amb aquestes definicions, cap dubte pot generar la qualificació com a dada personal de la informació relativa a les adreces de correu electrònic de les persones que treballen a l'empresa pública. Per tant, el seu tractament estarà subjecte als principis i obligacions de la normativa en matèria de protecció de dades."*

Per tot l'exposat, cap dubte hi pot haver que una adreça de correu corporatiu, en aquest cas, d'un Ajuntament, que utilitza en el seu format el primer cognom, la inicial del segon cognom i la inicial del nom, així com la identificació de la corporació, atès que permet la identificació del titular del compte, és una dada de caràcter personal protegida pels principis i garanties de la normativa de protecció de dades (RGPD i LOPDGDD).

III

Dit això, des del punt de vista de la protecció de dades cal tenir en compte que a l'Ajuntament, com a responsable del tractament de la informació personal de què disposa (article 4.7 RGPD), li correspon la tasca general de garantir que els tractaments de dades que s'efectuen a través dels seus sistemes d'informació i dels dispositius que facilita al seu personal per a l'exercici de les seves funcions professionals, s'adeqüen a la normativa de protecció de dades, i ha d'estar en disposició de demostrar aquest compliment, en aplicació del principi de responsabilitat proactiva (article 5.2 RGPD).

Això requereix que l'Ajuntament, en el cas que ens ocupa, dugui a terme una sèrie d'actuacions (article 24 RGPD), entre d'altres:

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

Aspectes aquests que, a més, s'han de plantejar no només respecte les dades personals de persones físiques, de què disposa l'Ajuntament per a l'exercici de llurs competències, sinó

també respecte les dades personals dels propis treballadors municipals que empren els sistemes d'informació i altres eines corporatives per desenvolupar les tasques professionals que tenen encomanades.

El responsable ha de tenir en consideració les implicacions que, per a la privacitat i la protecció de dades d'aquests empleats municipals i, si escau, de terceres persones, pot comportar l'establiment de mesures de control sobre l'ús de les eines esmentades per part del consistori, en aplicació del marc normatiu vigent, i de criteris per a un ús correcte d'aquests instruments.

Segons 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."

Així mateix, fem avinent que l'Esquema Nacional de Seguretat (ENS), aprovat pel Reial decret 311/2022, de 3 de maig, resulta d'aplicació, entre d'altres, a les administracions locals de conformitat amb la disposició addicional primera de l'LOPDGDD. L'article 12 del RD esmentat defineix la política de seguretat (apartat 1), i determina que cada administració pública ha de comptar amb una política de seguretat formalment aprovada per l'òrgan competent que reguli l'ús dels equips (apartat 3.2 i 5.8.1 de l'Annex II).

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'Ajuntament, en aquest cas, del compliment per part del seu personal 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 (...)".

Així doncs, el marc normatiu aplicable estableix la possibilitat que l'empresari, en el cas que ens ocupa, un Ajuntament, exerceixi un control o supervisió de l'ús que el seu personal fa dels mitjans de què disposa en l'àmbit laboral, amb les limitacions que es deriven del dret a la intimitat i a la dignitat del personal, tal com concreta reiterada jurisprudència, entre d'altres, en les SSTEDH de 5 de setembre de 2017 (cas Barbulescu) de 28 de febrer de 2018 (cas Libert); en les SSTC 241/2012, 170/2013, o 61/2021; o les SSTS 119/2018, de 8 de febrer, o 489/2018, de 23 d'octubre.

En síntesi, la jurisprudència 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 veure's afectats negativament per determinats usos, i també 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.

Ara bé, l'empresa ha de concretar aquestes normes d'ús de les dites eines, i informar-ne adequadament als treballadors.

Segons 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 determinados 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."*

Als efectes que interessen, serà en base a la normativa de protecció de dades i altra normativa esmentada, tenint en compte la jurisprudència rellevant i, si escau, les indicacions

i instruccions sobre els usos adequats de les eines de treball i comunicació que hagi establert l'Ajuntament, que pot determinar-se la licitud o il·licitud d'aquest ús en cada cas concret i, si escau, les responsabilitats que se'n puguin derivar.

IV

La consulta es refereix a enviaments de correus electrònics per part d'un treballador a d'altres treballadors de la corporació, "tractant temes sobre la mateixa", posant en còpia una adreça de correu externa a la corporació, sense consentiment d'aquests altres treballadors (que no haurien autoritzat, segons la consulta, que la seva adreça sigui coneguda pel destinatari extern del consistori). La consulta també es refereix al mateix supòsit, però utilitzant el dit treballador (emissor del missatge) una "adreça de correu personal".

L'RGPD disposa que tot tractament de dades personals ha de ser lícit (article 5.1.a)) i, en aquest sentit, estableix un sistema de legitimació del tractament de dades que es fonamenta en la necessitat de que concorri alguna de les bases jurídiques establertes al seu article 6.1, entre d'altres:

> *"1.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*
>
> *a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*
> *b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;*
> *c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;*
> *d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;*
> *e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*
> *(...)."*

Per tant, el tractament de dades personals que es produeixi arran de l'enviament de missatges de correu electrònic per part d'un treballador públic, serà lícit, d'entrada, en funció que concorri una o més bases jurídiques que habilitin el dit tractament.

Òbviament, el consentiment de les persones afectades (com serien, atesos els termes de la consulta, els titulars de les adreces electròniques corporatives incloses en el missatge, que es consideraria dada personal), podria ser base jurídica legitimadora del tractament (art. 6.1.a) RGPD).

Ara bé, tal i com posa de manifest el Grup de Treball de l'Article 29 (actualment, Comitè Europeu de Protecció de Dades), en el seu Dictamen 2/2017, sobre el tractament de dades en l'entorn laboral, la base jurídica per al tractament de dades en l'àmbit de les relacions laborals difícilment pot ser el consentiment -al menys, amb caràcter general-, atès que ens trobem en un context de desequilibri clar entre l'afectat (treballador) i el responsable del tractament (empresa).

Segons aquest Dictamen: *"Es muy poco probable que el consentimiento constituya una base jurídica para el tratamiento de datos en el trabajo, a no ser que los trabajadores puedan negarse sin consecuencias adversas (...). Salvo en situaciones excepcionales, los empresarios tendrán que basarse en otro fundamento jurídico distinto del consentimiento, como la necesidad de tratar los datos para su interés legítimo. Sin embargo, un interés legítimo en sí mismo no es suficiente para primer sobre los derechos y libertades de los trabajadores"*

En l'àmbit laboral, el tractament de les dades dels treballadors troba la seva justificació principalment en altres bases jurídiques diferents al consentiment dels afectats, com pot ser l'execució del contracte del que és part el treballador, que habilitaria el seu tractament per part de l'empresa (art. 6.1.c) RGPD), o el compliment d'una missió realitzada en interès públic o en exercici dels poders públics, en aquest cas, de l'Ajuntament (art. 6.1.e) RGPD).

Aquestes previsions poden habilitar, en termes generals, l'enviament de correus per part d'un treballador del consistori a d'altres persones (ja siguin altres treballadors o, si escau, destinataris externs), si aquest tractament de les dades de contacte corporatives es justifica en el desenvolupament de la seva feina, o guarda relació amb aquesta.

A això cal afegir que segons l'article 2.b) de la Llei 19/2014, de 29 de desembre, de transparència, accés a la informació pública i bon govern (LTC), és informació pública "la informació elaborada per l'Administració i la que aquesta té en el seu poder com a conseqüència de la seva activitat o de l'exercici de les seves funcions, inclosa la que li subministren els altres subjectes obligats d'acord amb el que estableix aquesta llei".

Les adreces de correu corporatiu dels empleats públics (i, si escau, altres dades de contacte professional), serien informació pública als efectes de la legislació de transparència.

Segons l'article 70.2 del Decret 8/2021, de 9 de febrer, sobre la transparència i el dret d'accés a la informació pública: *"Als efectes del que preveu l'article 24.1 de la Llei 19/2014, del 29 de desembre, són dades personals merament identificatives les consistents en el nom i cognoms, el càrrec o lloc ocupat, cos i escala, les funcions desenvolupades i el telèfon i les adreces, postal i electrònica, de contacte professional, referides al personal al servei de les administracions públiques, alts càrrecs i personal directiu del sector públic de les administracions públiques."*

Així, en principi no sembla que els treballadors hagin de tenir una expectativa de privacitat respecte l'ús de les adreces electròniques corporatives per part d'altres treballadors.

Això, sempre que les dades de contacte professional de tercers s'emprin, com s'ha apuntat, per al desenvolupament de l'àmbit propi i habitual de les relacions laborals, i sens perjudici del marge que, per a l'ús privat o particular de les eines de comunicació, hagi pogut establir l'empresa, qüestió a la que també ens hem referit.

Per tot l'exposat, les adreces de correu corporatives, com a dades de contacte professional, poden ser objecte de tractament amb motiu de comunicacions relacionades amb l'àmbit laboral, sempre que concorri una base jurídica habilitadora (art. 6.1 RGPD), i el seu ús resulti respectuós amb la resta de principis i garanties de la normativa de protecció de dades, en concret, el principi de finalitat, segons el qual les dades personals han de ser recollides amb

finalitats determinades, explícites i legítimes, i no han de ser tractades ulteriorment de manera incompatible amb aquestes finalitats (art. 5.1.b) RGPD).

Això, sens perjudici de les previsions que l'Ajuntament, en aquest cas, hagi determinat prèviament en relació amb l'ús adequat de les eines que posa a disposició dels treballadors, que aquests han de conèixer en els termes de la normativa esmentada.

Serà, doncs, en atenció al motiu i circumstàncies en què es produeixi una concreta comunicació de dades de contacte de treballadors municipals a un tercer destinatari extern al consistori, que es podrà determinar si aquesta comunicació resulta habilitada o, si escau, si es pot haver incorregut en un tractament inadequat d'aquestes dades de contacte professional.

V

En aquest context, vistos els termes en què es formula la consulta, cal apuntar que el mer fet d'incloure un destinatari que no formi part del propi Ajuntament no seria, *per se*, contrari a la normativa de protecció de dades.

Ans al contrari, a tall d'exemple pot ser fins i tot habitual que en una tramesa s'hagi de posar en còpia altres treballadors del consistori o d'altres administracions, ens públics o privats implicats en la prestació d'un servei, adreces de ciutadans o altres destinataris externs, etc.

Qüestió diferent seria, per exemple, la inclusió d'una adreça (no només d'un destinatari extern, sinó d'un destinatari de la pròpia corporació, per exemple, o d'una altra administració o entitat), de forma errònia, o sense que respongui a una finalitat legítima, i més, si això suposa posar en coneixement de tercers determinada informació personal a la que no haurien hagut de tenir accés tots o algun dels destinataris, en atenció al contingut del missatge en qüestió.

A efectes il·lustratius, fem notar que aquesta Autoritat ha examinat en diverses ocasions supòsits relatius a la tramesa de missatges de correu electrònic, des de la perspectiva de la protecció de dades, en els que s'ha analitzat les circumstàncies particulars de cada cas, als efectes de determinar tant la possible concurrència d'infracció a la normativa de la protecció de dades, com la determinació de les possibles responsabilitats (a tall d'exemple, esmentem la Resolució del procediment sancionador PS 33/2019, o la Resolució d'arxiu IP 340/2018, que es poden consultar al web www.apdcat.cat, ambdues relatives a la utilització del correu corporatiu). Anàlisi que no correspon dur a terme en aquest dictamen en relació amb el supòsit de la consulta, que s'exposa en termes generals.

En qualsevol cas, atesos els termes en què es formula la consulta, no es pot determinar si concorreria una infracció específica de la normativa de protecció de dades, pel mer fet d'haver-se produït un enviament d'un correu electrònic a un destinatari extern del consistori.

Caldrà examinar en cada cas si la inclusió d'un destinatari extern resulta lícit als efectes del principi de finalitat (art. 5.1.b) RGPD) i si concorre una base jurídica que habiliti el dit tractament (art. 6 RGPD).

Finalment, la consulta també es refereix al mateix supòsit, però en el cas d'utilitzar una adreça de correu particular del treballador (diferent de l'adreça corporativa que l'empresa subministra).

Pel que fa a aquesta circumstància, i partint de la base de les consideracions ja fetes, no podem descartar que, en l'àmbit laboral, puguin donar-se circumstàncies que justifiquin l'enviament d'un correu electrònic per part d'un treballador, no a través de l'adreça corporativa (que seria el supòsit habitual atès que és l'eina que l'empresa subministra al treballador amb aquesta finalitat), sinó des d'una adreça particular o personal del treballador.

Així, merament a tall d'exemple, poden donar-se circumstàncies en què el treballador es trobi amb la impossibilitat d'utilitzar l'adreça corporativa, i hagi de trametre un determinat missatge a través d'altres mitjans (per dificultats tècniques, per no disponibilitat de les eines de treball habituals per diferents motius, per trobar-se de vacances, en situació de teletreball, etc).

Aquest fet, en sí mateix, no sembla que hagi de constituir en qualsevol cas una infracció de la normativa de protecció de dades, sempre que es doni compliment als principis i garanties de protecció de dades a què ens hem referit.

Això, sens perjudici que s'hagi explicitat prèviament i de forma transparent una prohibició en aquest sentit per part de l'empresa (en aquest cas, l'Ajuntament), a través de la normativa d'ús de les eines corporatives i altres eines de comunicació per part del personal.

En qualsevol cas, per determinar aquest extrem caldrà tenir en compte les concretes directrius o indicacions que l'Ajuntament hagi especificat en relació amb aquesta possibilitat. Directrius que, com ha quedat dit, l'Ajuntament haurà d'haver posat necessàriament en coneixement dels treballadors, segons la normativa esmentada.

VI

Sens perjudici que, com es desprèn de les consideracions fetes, no correspon en aquest dictamen determinar si concorre o no una infracció de la normativa de protecció de dades en el supòsit concret, més enllà de les indicacions generals que s'han fet, convé apuntar el següent.

En supòsits concrets, la comissió d'una infracció de la normativa de protecció de dades pot ser atribuïble materialment a una persona concreta que presta serveis en una organització.

Ara bé, segons el sistema de responsabilitat previst a l'RGPD, la responsabilitat per les infraccions a la normativa de protecció de dades recau, entre d'altres, en els responsables del tractament, i no sobre els seus empleats.

Així, segons l'article 70.1 de l'LOPDGDD:

> *"Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:*
>
> *a) Los responsables de los tratamientos.*

b) Los encargados de los tratamientos.

(...).”

Com ha fet avinent aquesta Autoritat, entre d'altres, en les Resolucions dels procediments sancionadors PS 46/2021, PS 23/2020, o PS 33/2019, disponibles al web de l'Autoritat (www.apdcat.cat), d'acord amb el règim de responsabilitat previst a la normativa de protecció de dades, l'atribució de responsabilitat, si escau, per la comissió d'una infracció tipificada a la dita normativa per part del personal propi d'una entitat (articles 71 i ss. LOPDGDD), recauria en el responsable del tractament de dades.

Sobre això, cal tenir en compte la reiterada doctrina del Tribunal Suprem sobre l'atribució de responsabilitat quan la infracció la comet el personal d'una persona jurídica, basant-se en l'existència d'una culpa *in eligendo* o *in vigilando,* entre d'altres, la STS de 196/2021, de 15 de febrer, o la STS188/2022, de 15 de febrer, ambdues en matèria de protecció de dades de caràcter personal, a les que ens remetem a efectes il·lustratius.

Òbviament, en cada cas caldrà examinar, atenent a les circumstàncies concurrents, si concorre el principi de culpabilitat, és a dir, la necessitat que existeixi dol o culpa en l'acció punitiva, que resulta aplicable al dret administratiu sancionador, d'acord amb el règim de responsabilitat que preveu l'article 28 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, al que ens remetem.

Així mateix, recordem que, segons disposa l'article 77 de l'LOPDGDD, relatiu al règim aplicable al tractament de què siguin responsables determinades categories de responsables o encarregats, entre d'altres, les entitats que integren l'Administració local (apartat 1.c):

“(...).

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. ***Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes*** *para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.”*

Així, no és descartable que, en el cas que l'enviament d'un correu electrònic per part d'un treballador pugui comportar (per les circumstàncies de la tramesa o pel contingut del missatge) una infracció a la normativa de protecció de dades que seria en principi atribuïble

al responsable, se'n puguin derivar conseqüències de tipus disciplinari, en relació amb el treballador que hagi pogut actuar de forma negligent o contrària al compliment de la dita normativa.

En darrera instància, recordar que, en cas que l'Ajuntament detecti un mal ús dels equips subministrats al personal que pugui ser constitutiu de delicte o falta, s'hauria de comunicar al Ministeri Fiscal.

Conclusió

L'adreça de correu corporatiu d'un Ajuntament, que utilitza en el seu format el primer cognom, la inicial del segon cognom i la inicial del nom, així com la identificació de la corporació, atès que permet la identificació del titular del compte, és una dada de caràcter personal protegida per la normativa de protecció de dades.

El tractament de dades personals que es produeixi arran de l'enviament de missatges de correu electrònic per part d'un treballador públic, en concret, la inclusió d'adreces de correu corporatives de tercers i la tramesa a un destinatari extern, pot ser lícit si concorre una base jurídica (art. 6.1 RGPD) i es dona compliment al principi de finalitat (art. 5.1.b) RGPD).

Segons el sistema de responsabilitat previst a l'RGPD, la responsabilitat per les infraccions a la normativa de protecció de dades recau en els responsables del tractament, sens perjudici que d'una infracció a la normativa de protecció de dades se'n puguin derivar conseqüències de tipus disciplinari, en relació amb el treballador que hagi pogut actuar de forma negligent o contrària al compliment de la dita normativa.

Barcelona, 25 d'abril de 2023