apdcat
Autoritat Catalana de Protecció de Dades

Dictamen en relación con la consulta formulada por un Ayuntamiento en relación con la consideración del correo electrónico corporativo como dato personal y las consecuencias de su uso para el remitente

Se presenta ante la Autoridad Catalana de Protección de Datos una consulta formulada por un Ayuntamiento, en la que se pide un dictamen a esta Autoridad en relación con la consideración del correo electrónico corporativo como dato personal, y las consecuencias que su uso puede tener para el remitente, en diversas situaciones.

Analizada la consulta, que se acompaña de informe de la Secretaría General del Ayuntamiento sobre la cuestión planteada, vista la normativa vigente aplicable, y de acuerdo con el informe de la Asesoría Jurídica se dictamina lo siguiente:

Y

(...)

II

La consulta pregunta, de entrada, si el correo corporativo formado por el primer apellido, inicial del segundo apellido e inicial del nombre, así como la identificación de la corporación a la que pertenece, se considera dato personal, protegido por la normativa de protección de datos.

Asimismo, la consulta pregunta lo siguiente:

> *"El envío de un correo electrónico por un miembro de la corporación a otro miembro o miembros de la corporación, tratando temas sobre la misma, y poniendo en copia una dirección de correo de fuera de la corporación, sería susceptible de incurrir ¿en vulneración de la normativa sobre protección de datos? Qué consecuencias o acciones se pueden interponer en este supuesto, frente a la persona que forma parte de la corporación y titular de la cuenta de correo corporativo, que ha realizado el envío (remitente) al correo de otros miembros de la corporación, poniendo en copia ¿una dirección de correo electrónico de fuera de la corporación? ¿Ha incurrido el remitente en alguna infracción de la normativa sobre protección de datos?*
>
> *La misma situación, pero en caso de que el envío se hiciera, por un miembro de la corporación, pero desde su dirección de correo personal, ¿podría incurrir en vulneración de la normativa sobre protección de datos? ¿qué consecuencias o acciones se podrían interponer frente a dicha persona?"*
>
> La consulta añade que, en ambos casos, el envío sobre lo que se pregunta es siempre *"sin el consentimiento del destinatario o destinatarios del correo miembros de la corporación de facilitar su dirección de correo electrónico a un tercero, no miembro de la corporación".*

Situada la consulta en estos términos, es necesario partir de la base de que, según el artículo 4.1) del Reglamento (UE) 2016/679, de 27 de abril, general de protección de datos (RGPD), son datos de carácter 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 número, un número de identificación, datos de localización, un identificador online o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;".*

Por tanto, de entrada, cualquier información que permita identificar directa o indirectamente a una persona física es dato personal, y queda protegida por los principios y garantías de la normativa de protección de datos (RGPD y Ley orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales (LOPDGDD).

Según el considerante 26 del 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. (...)."*

A efectos de este dictamen resultan de especial interés la Recomendación 1/2013 de la Autoridad Catalana de Protección de Datos, sobre el uso del correo electrónico en el ámbito laboral, así como el *"Manual de buen uso del correo electrónico. Guía para las personas trabajadoras para la protección de la privacidad en el uso del correo electrónico",* disponibles en la web de la Autoridad (www.apdcat.cat).

Según la citada Recomendación (apartado 2), una dirección de correo electrónico puede definirse como *"el conjunto de palabras o signos que identifican al emisor o receptor de un mensaje de correo electrónico. Se elabora a partir de un conjunto de palabras o signos libremente escogidos, normalmente, por su titular o por la organización a la que pertenece, con el único límite de que esta dirección no coincida con la de otra persona. Está formada por una identificación del usuario, seguida del signo @ y, a continuación, el dominio (identificación facilitada por el proveedor del servicio de correo, con un punto, y unas siglas que pueden identificar la actividad de la organización (p .ej. ".org ") o las siglas del país (p. ej. ".es" o ".cat").*

Tal y como expone la Recomendación, podemos distinguir diferentes tipos de direcciones:

- Direcciones personalizadas: direcciones que contienen directamente información sobre su titular. Habitualmente, en las direcciones personalizadas se puede utilizar el nombre y apellidos completo, sólo las iniciales, o la inicial del nombre y apellido, etc. Estas direcciones de correo electrónico identifican directamente al titular del cuenta y por tanto debe considerarse como dato de carácter personal.

- Direcciones no personalizadas: son aquellas que, aunque se trata de una dirección vinculada a una cuenta de correo de una persona física determinada, no contienen información sobre su
titular (utilizan una combinación alfanumérica abstracta o sin significado alguno). En este caso, la dirección por sí sola no identificaría a la persona que es titular. Pero esta persona puede ser fácilmente identificable, sin un esfuerzo desproporcionado, bien porque la

dirección puede aparecer junto con otros datos que permiten su identificación, bien por el contenido del mensaje, bien a través de los datos de que dispone el servidor de correo. Por tanto, esta dirección también sería dato de carácter personal.

- Direcciones de correo electrónico genéricas: son las que responden a una cuenta genérica, de uso compartido o de un área de la organización (por ejemplo, consultes@empresa.cat). En este caso, la dirección de correo electrónico no puede vincularse a una persona física identificada o identificable, sino que pueden atenderla habitualmente usuarios diferentes. Por tanto, no se puede considerar dato de carácter personal.

En línea con ello, como recuerda esta Autoridad en varios informes (CNS 55/2019, IAI 18/2019, IAI 2/2021, o CNS 36/2022, que se pueden consultar en la web del Ayuntamiento), las direcciones de correo electrónico laborales o profesionales que pueden asociarse a personas físicas identificables (art. 4.1 RGPD), deben considerarse como dato de carácter personal.

Como se recuerda en el Dictamen CNS 4/2011 *"Hay que tener en cuenta que una dirección de correo electrónico aparecerá siempre necesariamente vinculada a un dominio concreto, de tal modo que es posible proceder a la identificación de su titular mediante la consulta del servidor en que se gestione este dominio, sin que ello requiera un esfuerzo desproporcionado por quien procede a la identificación. Por otra parte, las direcciones de correo electrónico de los trabajadores de una empresa (pública, en este caso) normalmente se configuran de tal modo (nombre_apellido@nombre del dominio) que fácilmente permiten identificar a sus titulares. Por tanto, de acuerdo con estas definiciones, ninguna duda puede generar la calificación como dato personal de la información relativa a las direcciones de correo electrónico de las personas que trabajan en la empresa pública. Por tanto, su tratamiento estará sujeto a los principios y obligaciones de la normativa en materia de protección de datos."*

Por todo lo expuesto, ninguna duda puede haber que una dirección de correo corporativo, en este caso, de un Ayuntamiento, que utiliza en su formato el primer apellido, la inicial del segundo apellido y la inicial del nombre, así como la identificación de la corporación, dado que permite la identificación del titular de la cuenta, es un dato de carácter personal protegido por los principios y garantías de la normativa de protección de datos (RGPD y LOPDGDD).

III

Dicho esto, desde el punto de vista de la protección de datos debe tenerse en cuenta que al Ayuntamiento, como responsable del tratamiento de la información personal de que dispone (artículo 4.7 RGPD), le corresponde la tarea general de garantizar que los tratamientos de datos que se efectúan a través de sus sistemas de información y de los dispositivos que facilita a su personal para el ejercicio de sus funciones profesionales, se adecuan a la normativa de protección de datos, y debe estar en disposición de demostrar este cumplimiento, en aplicación del principio de responsabilidad proactiva (artículo 5.2 RGPD).

Esto requiere que el Ayuntamiento, en caso de que nos ocupa, lleve a cabo una serie de actuaciones (artículo 24 RGPD), entre otras:

- La realización de un análisis de riesgos.
- La definición de una política de uso de los sistemas de información y dispositivos digitales.
- La implantación de medidas de seguridad técnicas y organizativas apropiadas al riesgo.

Aspectos estos que, además, deben plantearse no sólo respecto a los datos personales de personas físicas, de que dispone el Ayuntamiento para el ejercicio de sus competencias, sino también respecto a los datos personales de los propios trabajadores municipales que emplean los sistemas de información y otras herramientas corporativas para desarrollar las tareas profesionales que tienen encomendadas.

El responsable debe tener en consideración las implicaciones que, para la privacidad y la protección de datos de estos empleados municipales y, en su caso, de terceras personas, puede comportar el establecimiento de medidas de control sobre el uso de las herramientas citadas por parte del consistorio, en aplicación del marco normativo vigente, y de criterios para un uso correcto de estos instrumentos.

Según el artículo 87 de la LOPDDDD:

"1. Los trabajadores y 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 derechos reconocidos constitucional y legalmente. En su elaboración habrán de 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 que se refiere este apartado."

Asimismo, recuerda que el Esquema Nacional de Seguridad (ENS), aprobado por Real Decreto 311/2022, de 3 de mayo, resulta de aplicación, entre otros, a las administraciones locales de conformidad con la disposición adicional primera del LOPDDDD. El artículo 12 del citado RD define la política de seguridad (apartado 1), y determina que cada administración pública debe contar con una política de seguridad formalmente aprobada por el órgano competente que regule el uso de los equipos (apartado 3.2 y 5.8 .1 del Anexo II).

También es necesario tener en cuenta diversas previsiones de la normativa de ámbito laboral, en relación con la licitud de las medidas de control por parte del Ayuntamiento, en este caso, del cumplimiento por parte de su personal de sus obligaciones laborales.

Especialmente, el artículo 52 del Texto refundido de la Ley del Estatuto básico del trabajador público (TRLEBEP), aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, según el cual "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 (...)",* y el artículo 20.3 del Texto refundido de la Ley del Estatuto de los Trabajadores (ET), aprobado por el Real decreto legislativo 2/2015, de 23 de octubre, según el cual "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 (...)".*

Así pues, el marco normativo aplicable establece la posibilidad de que el empresario, en caso de que nos ocupa, un Ayuntamiento, ejerza un control o supervisión del uso que su personal hace de los medios de que dispone en el ámbito laboral, con las limitaciones que se derivan del derecho a la intimidad ya la dignidad del personal, tal y como concreta reiterada jurisprudencia, entre otras, en las SSTEDH de 5 de septiembre de 2017 (caso Barbulescu) de 28 de febrero de 2018 (caso Libert); en las SSTC 241/2012, 170/2013, o 61/2021; o las SSTS 119/2018, de 8 de febrero, o 489/2018, de 23 de octubre.

En síntesis, la jurisprudencia ha admitido que el empresario puede establecer controles sobre el uso de las herramientas que pone a disposición de las personas trabajadoras para la necesidad de coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencias de los trabajadores, para la protección de los sistemas de información, que pueden verse afectados negativamente por determinados usos, así como para la prevención de las responsabilidades que para el empresario puedan derivarse de formas ilícitas de uso frente a terceras personas.

Ahora bien, la empresa debe concretar estas normas de uso de dichas herramientas, informando adecuadamente a los trabajadores.

Según la STS de 26 de septiembre 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 estos usos; expectativa de 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 eso, ***lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de estos medios –con aplicación de prohibiciones absolutas o parciales– e informar a los trabajadores de que existió control y de los*** *medios que deben aplicarse con vistas a comprobar la corrección de los usos, así como de* ***las medidas que deben adoptarse*** *en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjudicio de la posible aplicación de otras medidas de carácter preventivo , como la exclusión de determinadas conexiones. De este modo,* ***si el medio se utiliza para usos privados en contra de estas prohibiciones y conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el***

control, se ha vulnerado «una expectativa raonable 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 ."*

A los efectos que interesen, será en base a la normativa de protección de datos y otra normativa mencionada, teniendo en cuenta la jurisprudencia relevante y, en su caso, las indicaciones e instrucciones sobre los usos adecuados de las herramientas de trabajo y comunicación que haya establecido Ayuntamiento, que puede determinarse la licitud o ilicitud de este uso en cada caso concreto y, en su caso, las responsabilidades que se puedan derivar.

IV

La consulta se refiere a envíos de correos electrónicos por parte de un trabajador a otros trabajadores de la corporación, "tratando temas sobre la misma", poniendo en copia una dirección de correo externa a la corporación, sin consentimiento de estos otros trabajadores (que no habrían autorizado, según la consulta, que su dirección sea conocida por el destinatario externo del consistorio). La consulta también se refiere al mismo supuesto, pero utilizando dicho trabajador (emisor del mensaje) una "dirección de correo personal".

El RGPD dispone que todo tratamiento de datos personales debe ser lícito (artículo 5.1.a)) y, en este sentido, establece un sistema de legitimación del tratamiento de datos que se fundamenta en la necesidad de que concurra alguna de las bases jurídicas establecidas en su artículo 6.1, entre otros:

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 se parte o para la aplicación a petición del mismo 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;
(...)."

Por tanto, el tratamiento de datos personales que se produzca a raíz del envío de mensajes de correo electrónico por parte de un trabajador público, será lícito, de entrada, en función de que concurra una o más bases jurídicas que habiliten dicho tratamiento .

Obviamente, el consentimiento de las personas afectadas (como serían, dados los términos de la consulta, los titulares de las direcciones electrónicas corporativas incluidas en el mensaje, que se consideraría dato personal), podría ser base jurídica legitimadora del tratamiento (art. 6.1. a) RGPD).

Ahora bien, tal y como pone de manifiesto el Grupo de Trabajo del Artículo 29 (actualmente, Comité Europeo de Protección de Datos), en su Dictamen 2/2017, sobre el tratamiento de datos en el entorno laboral, la base jurídica para el tratamiento de datos en el ámbito de las relaciones laborales difícilmente puede ser el consentimiento -al menos, a todos los efectos-, dado que nos encontramos en un contexto de desequilibrio claro entre el afectado (trabajador) y el responsable del tratamiento (empresa).

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

En el ámbito laboral, el tratamiento de los datos de los trabajadores encuentra su justificación principalmente en otras bases jurídicas distintas al consentimiento de los afectados, como puede ser la ejecución del contrato del que es parte el trabajador, que habilitaría su tratamiento por parte de la empresa (art. 6.1.c) RGPD), o el cumplimiento de una misión realizada en interés público o en ejercicio de los poderes públicos, en este caso, del Ayuntamiento (art. 6.1.e) RGPD).

Estas previsiones pueden habilitar, en términos generales, el envío de correos por parte de un trabajador del consistorio a otras personas (ya sean otros trabajadores o, en su caso, destinatarios externos), si este tratamiento de los datos de contacto corporativos se justifica en el desarrollo de su trabajo, o guarda relación con éste.

A esto hay que añadir que según el artículo 2.b) de la Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTC), es información pública "la información elaborada por el Administración y la que ésta tiene en su poder como consecuencia de su actividad o del ejercicio de sus funciones, incluida la que le suministran los demás sujetos obligados de acuerdo con lo establecido en esta ley".

Las direcciones de correo corporativo de los empleados públicos (y, en su caso, otros datos de contacto profesional), serían información pública a efectos de la legislación de transparencia.

Según el artículo 70.2 del Decreto 8/2021, de 9 de febrero, sobre la transparencia y el derecho de acceso a la información pública: "A efectos de lo *previsto en el artículo 24.1 de la Ley 19/2014, de 29 de diciembre, son datos personales meramente identificativos los consistentes en el nombre y apellidos, el cargo o puesto ocupado, cuerpo y escala, las funciones desarrolladas y el teléfono y las direcciones, postal y electrónica, de contacto profesional, referidas al personal al servicio de las administraciones públicas, altos cargos y personal directivo del sector público de las administraciones públicas."*

Así, en principio no parece que los trabajadores deban tener una expectativa de privacidad respecto al uso de las direcciones electrónicas corporativas por parte de otros trabajadores.

Esto, siempre que los datos de contacto profesional de terceros se empleen, como se ha apuntado, para el desarrollo del ámbito propio y habitual de las relaciones laborales, y sin perjuicio del margen que, para el uso privado o particular de las herramientas de

comunicación, haya podido establecer la empresa, cuestión a la que también nos hemos referido.

Por todo lo expuesto, las direcciones de correo corporativas, como datos de contacto profesional, pueden ser objeto de tratamiento con motivo de comunicaciones relacionadas con el ámbito laboral, siempre que concurra una base jurídica habilitadora (art. 6.1 RGPD) , y su uso resulte respetuoso con el resto de principios y garantías de la normativa de protección de datos, en concreto, el principio de finalidad, según el cual los datos personales deben ser recogidos con finalidades determinadas, explícitas y legítimas, in o deben ser tratadas ulteriormente de forma incompatible con estas finalidades (art. 5.1.b) RGPD).

Ello, sin perjuicio de las previsiones que el Ayuntamiento, en este caso, haya determinado previamente en relación con el uso adecuado de las herramientas que pone a disposición de los trabajadores, que éstos deben conocer en los términos de la citada normativa.

Será, pues, en atención al motivo y circunstancias en las que se produzca una concreta comunicación de datos de contacto de trabajadores municipales a un tercer destinatario externo al consistorio, que podrá determinarse si esta comunicación resulta habilitada o, en su caso, si puede haber incurrido en un tratamiento inadecuado de estos datos de contacto profesional.

V

En este contexto, vistos los términos en los que se formula la consulta, cabe apuntar que el mero hecho de incluir un destinatario que no forme parte del propio Ayuntamiento no sería, por sí, contrario a la normativa de protección de *datos* .

Al contrario, a modo de ejemplo puede ser incluso habitual que en un envío deba ponerse en copia otros trabajadores del consistorio o de otras administraciones, entes públicos o privados implicados en la prestación de un servicio, direcciones de ciudadanos u otros destinatarios externos, etc.

Cuestión distinta sería, por ejemplo, la inclusión de una dirección (no sólo de un destinatario externo, sino de un destinatario de la propia corporación, por ejemplo, o de otra administración o entidad), de forma errónea, o sin que responda a una finalidad legítima, y más, si ello supone poner en conocimiento de terceros determinada información personal a la que no habrían tenido que tener acceso todos o alguno de sus destinatarios, en atención al contenido del mensaje en cuestión.

A efectos ilustrativos, hacemos notar que esta Autoridad ha examinado en varias ocasiones supuestos relativos al envío de mensajes de correo electrónico, desde la perspectiva de la protección de datos, en los que se han analizado las circunstancias particulares de cada caso , a efectos de determinar tanto la posible concurrencia de infracción a la normativa de la protección de datos, como la determinación de las posibles responsabilidades (a modo de ejemplo, mencionamos la Resolución del procedimiento sancionador PS 33/2019, o la Resolución de archivo IP 340/2018, que se pueden consultar en la web www.apdcat.cat , ambas relativas a la utilización del correo corporativo). Análisis que no corresponde llevar a cabo en este dictamen en relación con el supuesto de la consulta, que se expone en términos generales.

En cualquier caso, dados los términos en que se formula la consulta, no puede determinarse si concurriría una infracción específica de la normativa de protección de datos, por el mero hecho de haberse producido un envío de un correo electrónico a un destinatario externo del consistorio.

Habrá que examinar en cada caso si la inclusión de un destinatario externo resulta lícito a efectos del principio de finalidad (art. 5.1.b) RGPD) y si concurre una base jurídica que habilite dicho tratamiento (art. 6 RGPD).

Por último , la consulta también se refiere al mismo supuesto, pero en el caso de utilizar una dirección de correo particular del trabajador (diferente de la dirección corporativa que la empresa suministra).

Por lo que se refiere a esta circunstancia, y partiendo de la base de las consideraciones ya hechas, no podemos descartar que, en el ámbito laboral, puedan darse circunstancias que justifiquen el envío de un correo electrónico por parte de un trabajador , no a través de la dirección corporativa (que sería el supuesto habitual dado que es la herramienta que la empresa suministra al trabajador a tal fin), sino desde una dirección particular o personal del trabajador.

Así, meramente a modo de ejemplo, pueden darse circunstancias en las que el trabajador se encuentre con la imposibilidad de utilizar la dirección corporativa, y deba enviar un determinado mensaje a través de otros medios (por dificultades técnicas, por no disponibilidad de las herramientas de trabajo habituales por diferentes motivos, por encontrarse de vacaciones, en situación de teletrabajo, etc).

Este hecho, en sí mismo, no parece que deba constituir en cualquier caso una infracción de la normativa de protección de datos, siempre que se dé cumplimiento a los principios y garantías de protección de datos a los que nos hemos referido.

Esto sin perjuicio de que se haya explicitado previamente y de forma transparente una prohibición en este sentido por parte de la empresa (en este caso, el Ayuntamiento), a través de la normativa de uso de las herramientas corporativas y otras herramientas de comunicación por parte del personal.

En cualquier caso, para determinar este extremo será necesario tener en cuenta las concretas directrices o indicaciones que el Ayuntamiento haya especificado en relación con esta posibilidad. Directrices que, como ha quedado dicho, el Ayuntamiento deberá haber puesto necesariamente en conocimiento de los trabajadores, según la citada normativa.

VI

Sin perjuicio de que, como se desprende de las consideraciones hechas, no corresponde en este dictamen determinar si concurre o no una infracción de la normativa de protección de datos en el supuesto concreto, más allá de las indicaciones generales que se han hecho, conviene apuntar lo siguiente.

En supuestos concretos, la comisión de una infracción de la normativa de protección de datos puede ser materialmente atribuible a una persona concreta que presta servicios en una organización.

Ahora bien, según el sistema de responsabilidad previsto en el RGPD, la responsabilidad por las infracciones en la normativa de protección de datos recae, entre otros, en los responsables del tratamiento, y no sobre sus empleados.

Así, según el artículo 70.1 de la LOPDDDD:

> *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.*
>
> *(...).”*

Como recuerda esta Autoridad, entre otras, en las Resoluciones de los procedimientos sancionadores PS 46/2021, PS 23/2020, o PS 33/2019, disponibles en la web de la Autoridad (www.apdcat.cat), de acuerdo con el régimen de responsabilidad previsto en la normativa de protección de datos, la atribución de responsabilidad, en su caso, por la comisión de una infracción tipificada en dicha normativa por parte del personal propio de una entidad (artículos 71 y ss (LOPDGDD), recaería en el responsable del tratamiento de datos.

Al respecto, es preciso tener en cuenta la reiterada doctrina del Tribunal Supremo sobre la atribución de responsabilidad cuando la infracción la comete el personal de una persona jurídica, basándose en la existencia de una *culpa inelegiendo* o *in vigilando ,* entre otros, la STS de 196/2021, de 15 de febrero, o la STS188/2022, de 15 de febrero, ambas en materia de protección de datos de carácter personal, a las que nos remitimos a efectos ilustrativos.

Obviamente, en cada caso habrá que examinar, atendiendo a las circunstancias concurrentes, si concurre el principio de culpabilidad, es decir, la necesidad de que exista dolo o culpa en la acción punitiva, que resulta aplicable al derecho administrativo sancionador, de acuerdo con el régimen de responsabilidad previsto en el artículo 28 de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, al que nos remitimos.

Asimismo, recordamos que, según dispone el artículo 77 de la LOPDDDD, relativo al régimen aplicable al tratamiento del que sean responsables determinadas categorías de responsables o encargados, entre otras, las entidades que integran la Administración local (apartado 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 hubiera cometido.*

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, ya 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."*

Así, no es descartable que, en caso de que el envío de un correo electrónico por parte de un trabajador pueda comportar (por las circunstancias del envío o por el contenido del mensaje) una infracción a la normativa de protección de datos que sería en principio atribuible al responsable, pudieran derivarse consecuencias de tipo disciplinario, en relación con el trabajador que haya podido actuar de forma negligente o contraria al cumplimiento de dicha normativa.

En última instancia, recordar que, en caso de que el Ayuntamiento detecte un mal uso de los equipos suministrados al personal que pueda ser constitutivo de delito o falta, debería comunicarse al Ministerio Fiscal.

Conclusión

La dirección de correo corporativo de un Ayuntamiento, que utiliza en su formato el primer apellido, la inicial del segundo apellido y la inicial del nombre, así como la identificación de la corporación, dado que permite la identificación del titular de la cuenta, es un dato de carácter personal protegido por la normativa de protección de datos.

El tratamiento de datos personales que se produzca a raíz del envío de mensajes de correo electrónico por parte de un trabajador público, en concreto, la inclusión de direcciones de correo corporativas de terceros y el envío a un destinatario externo, puede ser lícito si concurre una base jurídica (art. 6.1 RGPD) y se da cumplimiento al principio de finalidad (art. 5.1.b) RGPD).

Según el sistema de responsabilidad previsto en el RGPD, la responsabilidad por las infracciones a la normativa de protección de datos recae en los responsables del tratamiento, sin perjuicio de que de una infracción a la normativa de protección de datos se puedan derivar consecuencias tipo disciplinario, en relación con el trabajador que haya podido actuar de forma negligente o contraria al cumplimiento de dicha normativa.

Barcelona, 25 de abril de 2023