apdcat
Autoritat Catalana de Protecció de Dades

Dictamen en relación con la consulta formulada por un ayuntamiento sobre la política de uso de los sistemas de información y comunicación del consistorio

Antecedentes

Se presenta ante la Autoridad Catalana de Protección de Datos un escrito de un ayuntamiento, planteando diversas cuestiones relacionadas con la política de uso de los sistemas de información y comunicación que está elaborando el consistorio.

En concreto, en relación con la regulación del acceso y la gestión de las direcciones personalizadas de correo electrónico corporativas, así como de las aplicaciones corporativas, se formulan las siguientes cuestiones:

A. (...) En la baja definitiva de una dirección corporativa personalizada de correo electrónico cuando la persona usuaria que tiene asignado el buzón deja de prestar servicios al Ayuntamiento, tenemos las siguientes consultas:

- *Es necesario elaborar un procedimiento interno que establezca las normas de uso de los sistemas de información en los que se informe del protocolo de bloqueo de la dirección corporativa personalizada de correo electrónico y de cómo se gestionará en caso de baja definitiva y debe informarse a las personas usuarias de este procedimiento?*
- *Es necesario crear un mensaje de respuesta automática previo al bloqueo de la dirección corporativa personalizada de correo electrónico que informe de la baja de la persona usuaria que tiene asignada la dirección corporativa personalizada y que indique otra dirección de contacto para la remisión de correos ?*
- *¿Se pueden redireccionar de forma automática los correos electrónicos entrantes de la dirección corporativa personalizada de correo electrónico de la persona que deja de prestar servicios en el Ayuntamiento a una nueva dirección?*
- *¿El Ayuntamiento puede recuperar, si es conveniente, los mensajes necesarios para garantizar el buen funcionamiento del servicio con carácter previo a que la persona usuaria deje de prestar servicios en el Ayuntamiento y en su presencia? Si esto no es posible, ¿se pueden recuperar los mensajes y cómo hacerlo?*
- *Se puede permitir a la persona usuaria de la dirección corporativa personalizada que dejará de prestar servicios en el Ayuntamiento recuperar mensajes personales antes de que se bloquee la cuenta de correo y que la persona ya no preste servicios.*
- *¿Durante cuánto tiempo debe conservarse la cuenta activa de la dirección corporativa personalizada de correo electrónico de la persona usuaria que ha dejado de prestar servicios para que no se pueda considerar como un período de tiempo poco razonable y desproporcionado?*

- *¿Se puede dejar la cuenta inactiva de la dirección corporativa personalizada de correo electrónico a partir del día siguiente a la fecha en la que la persona usuaria deja de prestar servicios en el Ayuntamiento?*
- *Se podría considerar adecuado a la normativa de protección de datos que la dirección corporativa personalizada de correo electrónico pueda estar activa durante el plazo de un mes y se haga constar un mensaje de respuesta automática en el que se haga referencia a que la persona ya no presta servicios a la corporación y que para cualquier tema pueden ponerse en contacto con el Ayuntamiento, haciendo constar el correspondiente teléfono o dirección de correo electrónico.*
- *Una vez pasado el plazo en que la dirección corporativa personalizada de correo electrónico pueda estar activa, ¿se eliminará o conservará bloqueada y, en su caso, durante cuánto tiempo?*
- *A partir de la fecha en la que deja de prestar servicios la persona usuaria, ¿se podría descargar el contenido del buzón de correo electrónico y mantenerlo bloqueado, a la vez que se da de baja la dirección corporativa personalizada de correo electrónico? Si la respuesta es afirmativa, ¿durante cuánto tiempo se debe conservar bloqueada esta información?*

***B.** (...) Sobre el acceso a una dirección corporativa personalizada de correo electrónico corporativa de personas usuarias del correo que se encuentran en situación de baja temporal en la prestación de servicios, tenemos las siguientes consultas:*

- *Cuando una persona usuaria del servicio de correo está en situación de baja temporal, ¿en qué situaciones y cómo el Ayuntamiento puede acceder al contenido de su dirección corporativa personalizada de correo electrónico?*

***C.** (...) Con anterioridad a la situación de teletrabajo cuando una persona usuaria de las aplicaciones estaba de baja no iba a trabajar a las instalaciones municipales y, por tanto, no accedía a las aplicaciones asignadas desde su ordenador de sobremesa. Con el teletrabajo esto ha cambiado y las personas usuarias pueden acceder estando de baja en las aplicaciones mediante los dispositivos corporativos asignados oa través de internet. Esto hace que se puedan producir accesos indebidos durante esta situación de baja y que sea necesario llevar a cabo un seguimiento de los accesos realizados para evitar posibles fugas de información y tenemos las siguientes consultas:*

- *Cuando una persona usuaria de las aplicaciones está en situación de baja temporal en la prestación de servicios, en qué situaciones y cómo puede el Ayuntamiento monitorizar un período de tiempo y acceder al registro de accesos de las aplicaciones a las que la persona usuaria está autorizada a acceder?*

***D.** (...) ¿Cuándo una persona usuaria deja de prestar servicios al Ayuntamiento puede solicitar copia de los correos electrónicos de su dirección personalizada de correo electrónico corporativo?"*

Analizada la consulta y la documentación que le acompaña, vista la normativa vigente aplicable, y de acuerdo con el informe de la Asesoría Jurídica emito el siguiente dictamen.

Fundamentos Jurídicos

Y

(...)

II

La consulta plantea diversas cuestiones relacionadas con la política de uso de los sistemas de información y comunicación del Ayuntamiento, que se encuentra en fase de elaboración.

Desde el punto de vista de la protección de datos es importante tener en cuenta que el Ayuntamiento, como responsable del tratamiento de la información personal de la que dispone (artículo 4.7) del Reglamento (UE) 2016/679, del Parlamento y del Consejo Europeo, de 27 de abril de 2016, General de Protección de Datos (en adelante, RGPD)), le corresponde la tarea de garantizar y poder demostrar que los tratamientos de datos que se efectúan a través de sus sistemas de información y dispositivos que facilita a su personal para el ejercicio de sus funciones profesionales se adecuan a la normativa de protección de datos (artículo 5.2 RGPD, relativo al principio de responsabilidad proactiva).

Esto, en términos prácticos, requiere, entre otras actuaciones (artículo 24 RGPD):

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

Aspectos que, cabe decir, deben plantearse no sólo respecto a los datos personales de los ciudadanos de que dispone el Ayuntamiento para el ejercicio de sus competencias, sino también respecto a los datos personales de los empleados municipales que emplean los sistemas de información y otras herramientas corporativas para desarrollar las tareas profesionales que tienen encomendadas.

Esto obliga al Ayuntamiento a tener también en consideración las implicaciones que, para la privacidad y la protección de datos de estos empleados municipales, puede comportar el establecimiento de medidas de control sobre el uso de las herramientas mencionadas por parte del consistorio , en aplicación al marco normativo vigente.

Sobre estas cuestiones, cabe mencionar el artículo 87 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD), que dispone lo siguiente:

> *"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."*

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 empresario -en este caso, el Ayuntamiento-, del cumplimiento por parte de las personas trabajadoras 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 (...)".*

Hacer notar que la jurisprudencia (a modo de ejemplo, la STS de 26 de septiembre de 2007 o la más reciente STC 61/2021 a la que nos remitimos) 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 ser afectados negativamente por determinados usos, y para la prevención de las responsabilidades que para el empresario puedan derivarse de formas ilícitas de uso frente a terceras personas.

Especialmente relevante es, en este sentido, la Sentencia del Tribunal Europeo de Derechos Humanos (TEDH), caso *Barbulescu* , de 5 de septiembre de 2017, en el que el TEDH establece determinados elementos a aplicar en este contexto. En síntesis, el TEDH hace referencia a la información que se debe dar a las personas trabajadoras respecto a las medidas que puede tomar el empresario para supervisar estas herramientas, en particular, las comunicaciones de los trabajadores; cuál es el alcance de la supervisión; o si el empresario ha valorado la existencia de medidas de control menos intrusivas para las personas trabajadoras , entre otros (apartado 210 de la STEDH de 5 de septiembre de 2017, al que nos remitimos).

Recuerda también que esta Autoridad ha dictado la Recomendación 1/2013, sobre el uso del correo electrónico en el ámbito laboral (disponible en la web de la Autoridad), en la que se hacen diferentes consideraciones que resultan de especial interés en el caso examinado, ya las que haremos mención a lo largo de este dictamen.

III

Centrándonos en las cuestiones concretas planteadas en la consulta, buena parte de éstas están relacionadas con la regulación del acceso y la gestión de las cuentas de correo electrónico corporativas, con dirección personalizada, cuando se da de baja la dirección que tiene asignada una persona trabajadora con motivo de dejar de prestar servicios en el Ayuntamiento de forma definitiva.

De entrada, se plantea si " *hay que elaborar un procedimiento interno que establezca las normas de uso de los sistemas de información en los que se informe del protocolo de bloqueo de la dirección corporativa personalizada de correo electrónico y de cómo se gestionará en caso de baja definitiva"* , así como si " *hay que informar a las personas usuarias de este procedimiento".*

Tal y como se desprende del artículo 87.3 del LOPDDDD, transcrito en el apartado anterior, el Ayuntamiento debe contar con una política o manual que recoja los criterios o normas claras sobre las condiciones de uso de los sistemas de información y dispositivos digitales que pone a disposición de sus trabajadores para desarrollar sus funciones profesionales, las cuales deben advertir sobre los mecanismos de control sobre su uso que puedan afectar a la privacidad de las personas trabajadoras, las consecuencias que se pueden derivar de éste control y las garantías para las personas trabajadoras, en especial el derecho a ser informadas.

La previa información a las personas trabajadoras sobre estas cuestiones resulta primordial para poder considerar legítimo el control por parte del empresario respecto de las herramientas mencionadas y su uso (artículos 5.1.a) y 6 RGPD), como ha recordado ampliamente la jurisprudencia al respecto, como, entre otros, 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 ."*

Por su parte, el Esquema Nacional de Seguridad, aprobado por Real Decreto 311/2022, de 3 de mayo, que resulta de aplicación al Ayuntamiento de conformidad con la disposición adicional primera de la LOPDDDD, dispone, como a medida de seguridad, el establecimiento de normas de uso del correo electrónico para el personal de la organización (apartado 5.8).

Entre los distintos aspectos a tratar en estas normas o política de uso, sin duda sería conveniente recoger las medidas que se adoptarán para gestionar la cuenta personalizada de correo electrónico corporativo de las personas trabajadoras en caso de producirse el cese de su relación laboral con el Ayuntamiento.

Hay que tener presente que, desde el punto de vista de la protección de datos, la extinción de la relación laboral debe comportar el cese en el tratamiento de la información personal de la persona trabajadora por parte del Ayuntamiento y, por tanto, también de la dirección de la cuenta de correo electrónico personalizada que se le haya facilitado para el desarrollo de sus tareas profesionales, al extinguirse al mismo tiempo la finalidad que justificó su tratamiento (artículos 5.1 b) ye) RGPD, principios de limitación de finalidad y plazo de conservación, respectivamente).

Esto puede tener implicaciones tanto para la persona trabajadora, quien podría tener interés en disponer de los mensajes privados o personales de su cuenta corporativa, como para el propio Ayuntamiento, quien podría verse afectada la continuidad de la actividad municipal en mayor o menor medida.

Apuntar que, aunque se desconoce si en la política de uso que se está elaborando el Ayuntamiento prevé admitir cierto uso privado de las cuentas personalizadas de correo electrónico corporativas, hay que tener presente, como apunta esta Autoridad a la Recomendación 1/ 2013, antes citada, que incluso respecto a las cuentas de correo de las que se establezca un uso exclusivamente profesional la persona trabajadora no siempre podrá evitar, por ejemplo, el uso que hagan terceras personas de este correo, para remitirle mensajes de carácter personal.

A efectos de garantizar un correcto tratamiento de la información en estos casos, es importante disponer de un procedimiento interno relativo al uso del correo electrónico corporativo que tenga en cuenta ésta y otras circunstancias, y donde se informe de forma previa al bloqueo de la cuenta de la persona trabajadora de la gestión que realizará el Ayuntamiento y, por tanto, de las medidas concretas que se pueden adoptar en este sentido.

Recordar que la determinación y adopción de estas medidas es, en todo caso, una decisión que corresponde al Ayuntamiento, en atención a sus necesidades a la hora de tratar la información personal de la que es responsable (artículos 4.7 y 26 RGPD).

IV

En relación con las posibles medidas a adoptar, en la consulta se plantea si *"es necesario crear un mensaje de respuesta automática previo al bloqueo de la dirección corporativa personalizada de correo electrónico que informe de la baja de la persona usuaria que tiene asignada la dirección corporativa personalizada y que indique otra dirección de contacto para la remisión de correos"* y si *"se pueden redireccionar de forma automática los correos electrónicos entrantes de la dirección corporativa personalizada de correo electrónico de la persona que deja de prestar servicios en el Ayuntamiento en una nueva dirección".*

En el apartado III.4 de la Recomendación 1/2013, referido al acceso al correo electrónico por parte de la empresa (en este caso, el Ayuntamiento), se identifican algunas actuaciones que el empresario puede llevar a término para gestionar correctamente la información con motivo del cese de la relación laboral de la persona trabajadora.

En concreto, se apunta que en estas situaciones es necesario comunicarlo inmediatamente a la persona responsable de la gestión de las cuentas de correo electrónico para que *"se inutilicen los códigos de usuario y las contraseñas del trabajador y, en su caso, 'incluya un mensaje automático de respuesta para el correo entrante que indique la nueva dirección a la que se pueden dirigir los mensajes por razones profesionales."*

Por tanto, en atención a las necesidades concretas que puedan concurrir en el caso concreto (por ejemplo, según el puesto y/o cargo de la persona trabajadora y las funciones que viene desarrollando), puede resultar una medida adecuada programar un mensaje automático de respuesta para todos los correos entrantes en el buzón de la persona trabajadora que deja de prestar servicios en el Ayuntamiento, indicando que la

cuenta en cuestión está en desuso y la nueva dirección de correo corporativa donde se pueden dirigir los correos por motivos profesionales.

Esta actuación es preferible al reenvío de forma automática de los correos electrónicos entrantes a otra dirección de correo corporativa, dado que, en estos casos, se produce una carencia de control sobre los correos electrónicos en cuestión, por lo que la información privada que eventualmente pudiera constar podría acabar siendo conocida por personas no previstas por la persona remitente de la comunicación, pudiendo contravenir no sólo la normativa de protección de datos (artículo 5.1.e) RGPD, principio de integridad y confidencialidad), sino también otros derechos constitucionalmente protegidos (intimidad y secreto de las comunicaciones (artículo 18.1 y 3 CE)).

V

En la consulta también se plantea si *"el Ayuntamiento puede recuperar, si es conveniente, los mensajes necesarios para garantizar el buen funcionamiento del servicio con carácter previo a que la persona usuaria deje de prestar servicios en el Ayuntamiento y en su presencia "* y si esto no es posible *"si se pueden recuperar los mensajes y cómo se debe hacer".*

Tal y como indica esta Autoridad en la Recomendación 1/2013, uno de los objetivos que podría justificar el acceso al correo electrónico corporativo de las personas trabajadoras por parte del empresario, en este caso el Ayuntamiento, y siempre que se haya informado adecuadamente, es el de garantizar la continuidad de la actividad normal de la empresa, dado que ésta podría verse afectada en caso de no disponer de cierta información profesional (artículo 87 LOPDGDD, en conexión con la normativa laboral y la jurisprudencia existente) .

También en este caso, como se señala en dicha Recomendación, es conveniente planificar y definir en la política de uso de los sistemas de información -e informar a los trabajadores- las medidas que se adoptarán en este sentido en caso de ausencia de las personas trabajadoras y también en el caso de cese de la relación laboral (apartado III. 2 y 4).

Hacer notar que, en aplicación del principio de responsabilidad proactiva (artículo 5.2 RGPD), el responsable, en este caso, el Ayuntamiento, debe responder del cumplimiento de los principios de protección de datos y, por eso, no es suficiente alegar una finalidad para el acceso que en términos generales puede ser lícita, sino que debe motivarse en base a las circunstancias de cada caso.

Así, en el caso de cese de la relación laboral, y siguiendo las consideraciones formuladas en la Recomendación 1/2013, así como en la Recomendación CM/REC (2015) 5, de 1 de abril de 2015, del Comité de Ministros del Consejo de Europa, relativa al tratamiento de datos personales en el contexto de la relación de trabajo, podría establecerse en la política de uso que el acceso a la cuenta de correo electrónico corporativo de las personas trabajadoras que pudiera justificarse en esta finalidad de garantizar la continuidad de la actividad normal del Ayuntamiento tiene por finalidad recuperar la información vinculada estrictamente a la actividad profesional de la persona trabajadora que causa baja definitiva en el Ayuntamiento cuando ésta resulta esencial para continuar

con el actividad normal municipal; que el acceso se llevará a cabo, siempre que sea posible, con anterioridad al día en que se cesa efectivamente la relación laboral con el Ayuntamiento, ante la presencia de la persona trabajadora y, en su caso, de un tercero; que, cuando esto no sea posible, el órgano superior de la persona ex trabajadora tendrá que valorar de forma motivada la necesidad de la intervención y tendrá que identificar la información concreta a la que hay que acceder, y que el acceso se comunicará, si es posible, a la persona ex trabajadora; y que, en ningún caso, el acceso abarcará mensajes que puedan identificarse claramente como privados o personales, o bien aquellos que la propia persona trabajadora señale de esta naturaleza.

Hay que tener presente que, dadas las finalidades previstas en el artículo 87 de la LOPDDDD, en conexión con la normativa laboral examinada, que pueden habilitar el acceso y monitorización de los equipos que la empresa pone a disposición de sus trabajadores, el acceso a información privada no resultaría ni proporcionado ni justificado.

VI

En la consulta también se plantea si *"se puede permitir a la persona usuaria de la dirección corporativa personalizada que dejará de prestar servicios en el Ayuntamiento recuperar mensajes personales antes de que se bloquee la cuenta de correo y que la persona ya no preste servicios. "*

Tal como se recuerda en la Recomendación 1/2013 (aparado II.4), es importante establecer en la política de uso un plazo máximo de conservación de los mensajes privados, cumplido el cual deben borrarse, así como fomentar la creación de carpetas para almacenar correos de esta naturaleza que permitan su identificación fácilmente en caso de un eventual acceso por parte del empresario a la cuenta de correo corporativo.

También se recuerda en dicha Recomendación (apartado III.4) que, dado el caso de cese de la relación laboral, la empresa (el Ayuntamiento) debe facilitar a la persona trabajadora la obtención de los mensajes privados de dicha cuenta de correo corporativo, siempre que no superen el período máximo de conservación que se haya establecido en la política de uso. Y que, en este caso, el acceso debe producirse en presencia de la persona trabajadora para identificar los mensajes de carácter exclusivamente personal, quien podría decidir borrar estos mensajes privados o transferirlos a otra cuenta de correo.

VII

En la consulta se plantean también algunas cuestiones relacionadas con mantener activa durante un cierto tiempo la dirección personalizada de correo electrónico corporativa de la persona trabajadora que deja de prestar servicios al Ayuntamiento. En concreto:

- *"Durante cuánto tiempo debe conservarse la cuenta activa de la dirección corporativa personalizada de correo electrónico de la persona usuaria que ha dejado de prestar servicios para que no se pueda considerar como un período de tiempo poco razonable y desproporcionado."*

- *"Se puede dejar la cuenta inactiva de la dirección corporativa personalizada de correo electrónico a partir del día siguiente a la fecha en que la persona usuaria deja de prestar servicios en el Ayuntamiento"*
- *"Se podría considerar adecuado a la normativa de protección de datos que la dirección corporativa personalizada de correo electrónico pueda estar activa durante el plazo de un mes y se haga constar un mensaje de respuesta automática en el que se haga referencia a que la persona ya no presta servicios a la corporación y que para cualquier tema pueden ponerse en contacto con el Ayuntamiento, haciendo constar el correspondiente teléfono o dirección de correo electrónico."*
- *"Una vez pasado el plazo en que la dirección corporativa personalizada de correo electrónico pueda estar activa, debe eliminarse o conservarse bloqueada y, en su caso, durante cuánto tiempo ."*

Como se ha avanzado en el apartado III de este dictamen, desde el punto de vista de la protección de datos, la extinción de la relación laboral debe comportar el cese en el tratamiento de la información personal de la persona trabajadora por parte del Ayuntamiento y, por tanto, también de su cuenta de correo electrónico corporativo, al extinguirse la finalidad que justifica su tratamiento.

Ésta es una exigencia que deriva del principio de limitación de la finalidad (artículo 5.1.b) RGPD), según el cual *"las datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichas finas ; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de las datos personales con fines de archivo en interés público, fines de investigación científica e histórico o fines estadísticos no se considerará incompatible con los fines iniciales".*

Principio que debe ponerse en consonancia con el principio de limitación del plazo de conservación (artículo 5.1.e) RGPD), según el cual *"las 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 las datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se tratan exclusivamente finas de archivo en interés público, finas 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".*

Al respecto, según el considerante 39 del RGPD: "(…) *Las datos personales deben ser adecuadas, pertinentes y limitadas 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. Las datos personales sólo deben tratarse si la finalidad del tratamiento no pudiera conseguirse razonablemente por otros medios. Para garantizar que las datos personales no se conservan más tiempo del necesario, el responsable del tratamiento debe establecer plazos para su supresión o revisión periódica. (…)."*

Aparte de estos principios, resulta especialmente relevante el derecho de supresión regulado en el artículo 17 del RGPD, de acuerdo con el cual:

> *"1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de las datos personales que le conciernen, el cual*

estará obligado a suprimir sin dilación indebida las datos personales cuando concurra alguna de las circunstancias siguientes:
a) las 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 éste no se base en otro fundamento jurídico;
c) el interesado se oponga al tratamiento conforme al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento conforme al artículo 21, apartado 2;
d) las datos personales hayan sido tratados ilícitamente;
e) las 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) las 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.
(...).”

Se desprende de ello que el responsable del tratamiento (artículo 4.7 RGPD) debe conservar los datos personales durante el menor tiempo posible y que, en la determinación de este plazo de conservación, debe tenerse en cuenta la finalidad para la cual se necesita el tratamiento de los datos, de tal forma que, una vez alcanzada la finalidad, los datos personales tendrán que ser suprimidos. También debería tenerse en cuenta las obligaciones de conservación de los datos durante un tiempo determinado que puedan establecer disposiciones aplicables, de tal forma que, cumplidos estos plazos, es cuando los datos personales deberán suprimirse.

Tal y como dispone la propia normativa de protección de datos, la supresión, cuando es pertinente, no equivale necesariamente al borrado o destrucción de la información personal, sino a su bloqueo.

En concreto, el artículo 32 de la LOPDDDD establece lo siguiente:

“1. El responsable del tratamiento estará obligado a bloquear las datos cuando proceda a su rectificación o supresión .
2. El bloqueo de las datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, salvo para la puesta a disposición de las 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 las datos.
3. Las 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 las datos durante el mismo.
(...).”

Así pues, los datos personales deben suprimirse una vez dejen de ser necesarios o pertinentes para la finalidad para la que se recogieron o, en su caso, una vez finalizados los plazos de conservación establecidos por la ley, lo que comportará su bloqueo durante los plazos de prescripción en los que pueda exigirse algún tipo de responsabilidad derivada del tratamiento. Cumplido este plazo, que puede variar en función de la información tratada y de las responsabilidades que pueden generarse, debe procederse a la eliminación efectiva de la información personal.

Esto trasladado al caso que nos ocupa, y dando así respuesta a las preguntas formuladas, implica que, con carácter general, la supresión (y, por tanto, bloqueo) de la dirección personalizada de correo electrónico corporativo de la persona trabajadora que deja de prestar servicios en el Ayuntamiento debería efectuarse en el momento en que se produce la extinción de la relación laboral (podría ser el día siguiente a la fecha en que deja de prestar servicios).

Ahora bien, con el fin, cuando proceda, de garantizar la continuidad del servicio, puede resultar admisible mantener "activa" la dirección corporativa en cuestión, a pesar de que la persona titular ya no preste servicios en el Ayuntamiento, durante cierto tiempo. Hacer notar que no todos los puestos de trabajo podrían justificar que se mantenga es la dirección operativa, dependerá del cargo o de las funciones que tenía asignadas la persona ex trabajadora.

Hay que tener presente que, en todo caso, esta actuación debería limitarse a la programación del mensaje de respuesta automática a que se ha mencionado en el apartado IV de este dictamen, en el que se informa a los remitentes de los correos entrantes que la cuenta en cuestión está en desuso y la dirección a la que deben dirigirse los mensajes en caso de querer contactar con el departamento o área municipal correspondiente.

Respecto al tiempo en que podría mantenerse con este objetivo activa la dirección de correo electrónico, hacer notar que no existe una previsión normativa en este sentido, si bien, en aplicación del principio de limitación de la conservación de los datos (artículo 5.1.e) RGPD), no debería alargarse más allá del tiempo estrictamente necesario para alcanzar la finalidad de no perder información relevante para el Ayuntamiento.

Como orientación, señalar que la Autoridad Belga de Protección de Datos recomienda un plazo de un mes a todos los efectos, que podría, en atención al contexto y las funciones o cargo que ostentaba la persona ex trabajadora, ampliarse hasta un máximo de tres meses (Decisión emitida el 29 de septiembre de 2020, disponible en su web).

Visto esto, la opción planteada en la consulta consistente en mantener activa la dirección durante el plazo de un mes y haciendo constar un mensaje de respuesta automática informando sobre la nueva dirección o teléfono de contacto de la persona a la que dirigirse se resultaría adecuada a la normativa de protección de datos.

Durante ese plazo en que esté en funcionamiento el mensaje de respuesta automática, el buzón de correo electrónico debería mantenerse bloqueado de tal forma que no se pueda acceder a su contenido.

A todo esto, la consulta plantea si *"a partir de la fecha en la que deja de prestar servicios la persona usuaria, se podría descargar el contenido del buzón de correo electrónico y mantenerlo bloqueado, a la vez que se da de baja la dirección corporativa personalizada de correo electrónico"* y, en caso afirmativo, *"durante cuánto tiempo se debe conservar bloqueada esta información."*

La normativa de protección de datos obliga al responsable del tratamiento (el Ayuntamiento) a bloquear los datos cuando lleve a cabo su supresión (artículo 32.1 LOPDGDD).

En un caso como el planteado, en el que se debe dar de baja la dirección personalizada de correo electrónico corporativo con motivo del cese de la relación laboral de la persona trabajadora, respecto al contenido del buzón (el conjunto de mensajes que se pueden contener), a fin de poder cumplir con esta obligación de bloqueo, sería razonable que a tal efecto esta información pudiera ser descargada o guardada por el responsable y conservarla debidamente bloqueada.

Teniendo en cuenta que se trata de una herramienta facilitada para el desarrollo de las tareas profesionales de las personas trabajadoras y vistas las pautas y recomendaciones que estas personas deben seguir cuando se admite un uso privativo de esta herramienta (configuración de los mensajes, organización en carpetas, respetar el período de conservación fijado, verificar periódicamente los que deben eliminarse, posibilidad de recuperar los mensajes antes del cese de la relación laboral, etc.), a priori en el buzón de correo electrónico corporativo no hay deberían constar mensajes de naturaleza privada o personal de la persona ahora ex trabajadora, si bien tampoco es posible descartarlo con toda seguridad. Lo mismo podría ocurrir a pesar de que la cuenta de correo corporativo se facilitara para motivos exclusivamente profesionales.

Por eso, como garantía adicional para el respeto a los derechos de la persona ex trabajadora, sería conveniente que antes de descargar el contenido del buzón se llevara a cabo una revisión de éste para detectar correos que, en atención al asunto, induzcan a pensar que se trata de mensajes de carácter privado o personales, o bien para localizar carpetas de almacenamiento de correos que puedan haberse identificado como privadas o personales, y borrarlo (sin acceder a su contenido).

Hecho esto, y una vez descargada la información, debe conservarse debidamente bloqueada y no se podrá tratar para ninguna finalidad, salvo para la puesta a disposición de los datos a los jueces y tribunales, al Ministerio Fiscal oa las administraciones públicas competentes , en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento (artículo 32.3 LOPDGDD).

El plazo durante el cual debe mantenerse la información bloqueada puede variar en función de su naturaleza y de las responsabilidades que se pueden generar y, una vez cumplido, deberá procederse a la eliminación efectiva de esta información (artículo 32.2 LOPDGDD).

VIII

La consulta también plantea *"cuando una persona usuaria del servicio de correo está en situación de baja temporal, en qué situaciones y cómo el Ayuntamiento puede acceder al contenido de su dirección corporativa personalizada de correo electrónico."*

Tal y como se pone de manifiesto en el apartado III.2 de la Recomendación 1/2013, la ausencia de un trabajador, especialmente si es de larga duración, puede comportar problemas para la continuidad de la actividad normal de la empresa, si no se puede acceder a una determinada cuenta
de correo.

La Autoridad pone el énfasis en la necesidad de planificar -y dejar constancia en la política de uso- las medidas que se adoptarán para garantizar la continuidad durante la ausencia de esta persona, de tal forma que no sea necesario l acceso del empresario a su cuenta de correo por el riesgo que ello puede comportar para los derechos de la persona trabajadora.

Entre estas medidas, puede preverse, a modo de ejemplo, que la persona trabajadora puede eliminar o trasladar a una carpeta personal todos los mensajes privados o de carácter personal, y autorizar el acceso a otro trabajador, adoptando los cambios pertinentes, tanto al inicio como fin del período en que cause baja, en lo que se refiere al cambio de las contraseñas; y/o transferir la información necesaria para continuar con la actividad durante su ausencia.

Si esto no es posible, por ejemplo en caso de ausencia imprevista de la persona trabajadora, es necesario que el órgano superior de la persona trabajadora ausente valore de forma motivada la necesidad de la intervención para la continuidad del servicio (necesidad improrrogable ligada actividad laboral).

También es necesario comunicar este acceso a la persona trabajadora con antelación, si es posible, o bien con carácter posterior cuando no haya sido posible (lo antes posible).

Este acceso debe realizarse en presencia o bajo la supervisión del órgano superior de la persona trabajadora y, en caso de que se le haya podido comunicar, con su asistencia o de la persona que designe la persona interesada, si lo desea .

No podrá accederse en ningún caso, por este motivo, a los mensajes que la persona trabajadora haya señalado como privados o que tenga almacenados en una carpeta identificada como privada o personal.

IX

Por otra parte, en la consulta se pone de manifiesto que, con anterioridad a la situación de teletrabajo, cuando una persona usuaria de las aplicaciones corporativas estaba de baja no iba a trabajar a las instalaciones municipales y, por tanto, no accedía a las aplicaciones asignadas desde su ordenador de sobremesa, pero que esto, con el

teletrabajo, ha cambiado y las personas usuarias pueden acceder estando de baja mediante los dispositivos corporativos asignados oa través de internet.

Esto, sostiene, hace que se puedan producir accesos indebidos durante esta situación de baja y que sea necesario llevar a cabo un seguimiento de los accesos realizados para evitar posibles fugas de información.

Visto esto, plantea *"cuando una persona usuaria de las aplicaciones está en situación de baja temporal en la prestación de servicios, en qué situaciones y cómo puede el Ayuntamiento monitorizar un período de tiempo y acceder al registro de accesos de las aplicaciones a las que la persona usuaria está autorizada a acceder."*

Recordar que corresponde al Ayuntamiento, como responsable, establecer en la política de uso que está elaborando los criterios generales y las normas que procedan para su adecuada utilización, no sólo del correo electrónico corporativo, sino también de sus sistemas de información, que pone a disposición de sus trabajadores para que éstos actúen con responsabilidad y estén informados del control que puede ejercer el Ayuntamiento en el uso de estos sistemas.

Teniendo en cuenta que el Ayuntamiento debe ser capaz de demostrar que el tratamiento de datos a través de sus sistemas de información se adecua a la normativa de protección de datos (artículo 5.2 RGPD), es necesario reconocerle la posibilidad de poder llevar a cabo, a través de las personas designadas por esta función, las tareas de control y seguimiento que sean necesarias en las infraestructuras comunes y en las estaciones de trabajo asignadas a su personal a efectos de comprobar y verificar que el uso de los sistemas de información y aplicaciones corporativas se ajusta a lo que establece la política de uso y no genera incidentes de seguridad.

Hacer notar que este tipo de control debe ser proporcionado al tipo de riesgo que pueda derivarse del mal uso de los sistemas de información para el Ayuntamiento o terceras personas por parte de todas aquellas personas que tienen autorizado el acceso a los sistemas de información información (no debería ser una medida pensada sólo para los trabajadores que se encuentran prestando servicios en la modalidad de teletrabajo y que se encuentran ausentes con motivo de una baja por enfermedad o de otra índole).

Visto esto, el Ayuntamiento podría establecer en la política de uso las limitaciones en el uso del correo electrónico y en los demás sistemas de información que sea necesario introducir durante el período en que se esté de baja, que, con la finalidad de garantizar el buen funcionamiento de los sistemas de información y de hacer un seguimiento de su adecuada utilización por parte de su personal, dispone de herramientas y medios de control para supervisar y realizar este seguimiento, los cuales, por ejemplo, permiten registrar acceso a los sistemas de información por parte de sus usuarios (identificación del usuario, día, hora, recurso al que se accede y motivo del acceso), y el período de tiempo en el que se revisará la información de control registrada (por ejemplo, una vez al mes).

Sería conveniente también de las posibles consecuencias en el caso de la existencia de indicios de un mal uso de los sistemas de información por parte de los trabajadores, por incumplir las normas.

X

Por último, en la consulta se plantea si *"cuando una persona usuaria deja de prestar servicios al Ayuntamiento puede solicitar copia de los correos electrónicos de su dirección personalizada de correo electrónico corporativo."*

Respecto a los correos de naturaleza privada o personal, como se ha visto, debería facilitarse el acceso de la persona trabajadora antes de su marcha definitiva del puesto de trabajo, si bien, ante una petición posterior de acceso a esta información, no debería haber, a priori, inconvenientes desde el punto de vista de la protección de datos, dado que se trataría de información a la que podría tener acceso en ejercicio de su derecho de acceso a la información que le es propia, en los términos del artículo 15 del RGPD.

Respecto a los correos profesionales, el artículo 15 del RGPD permitiría dar acceso a los datos directamente vinculados a la persona trabajadora (o mejor a su condición de persona remitente o receptora del mensaje) pero en cambio no parece que pueda abarcar el acceso a información de terceras personas que pueda constar en dichos correos.

Respecto a esta información hay que tener presente que se trataría de información que figuraría en poder del Ayuntamiento como consecuencia del ejercicio de las funciones encomendadas a la persona que pide su acceso. Por tanto, se trataría de información pública a los efectos del artículo 2.b) de la Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno (en adelante, LTC), y , consecuentemente, sometida al régimen del derecho de acceso (artículo 18 LTC).

El artículo 18 de la LTC reconoce el derecho de las personas a *"acceder a la información pública, a la que hace referencia el artículo 2.b, a título individual o en nombre y representación de cualquier persona jurídica legalmente constituida "* (apartado 1).

Ahora bien, debe tenerse en cuenta que este derecho de acceso no es absoluto y puede ser denegado o restringido por las causas expresamente establecidas en las leyes. A los efectos que interesan, debe tenerse presente que en los correos profesionales solicitados constará información propia de la persona ex trabajadora, a la que podría tener acceso en base al artículo 15 del RGPD, pero también y principalmente información de terceras personas. Esto obligaría a tener presente las limitaciones y criterios previstos en la legislación de transparencia (artículos 23 y 24 LTC), y los principios de la normativa de protección de datos personales.

Hacer notar, en este punto, que esta Autoridad ha tenido la oportunidad de examinar el eventual acceso y obtención de copia de los correos profesionales por parte de una persona ex trabajadora de un ente local en el informe IAI 2/2021 , disponible en la web de la Autoridad.

Tal y como se recuerda en este informe, en atención a las funciones que tuviera atribuidas la persona ex trabajadora, podríamos encontrarnos ante información que podría ser de diversa naturaleza y afectar en mayor o menor grado a la privacidad de las personas a las que hace referencia.

De entrada, el acceso de la persona solicitante y la obtención de una copia de los correos profesionales en los que se contengan datos personales especialmente protegidos de terceras personas, una vez finalizada su relación laboral con el Ayuntamiento, debería verse en todo caso limitado en base a lo previsto en los artículos 23 de la LTC y 15.1 de la *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno* (LTC)).

Pero más allá de esto, en el contenido de estos correos profesionales también podrían constar datos merecedores de una especial reserva o confidencialidad en atención a la concurrencia de determinadas circunstancias calificadas (por ejemplo, situaciones de vulnerabilidad social, datos de menores, datos relacionados con la violencia de género, etc.) o en atención a la naturaleza de los asuntos tratados por la persona ex trabajadora según sus tareas o funciones asignadas (miembros de la policía local, personal del área de servicios sociales, etc.).).

También habría que tener presente que el acceso pretendido podría afectar a un gran volumen de personas. Si bien el número de afectados no es propiamente un criterio decisivo a la hora de poder limitar el acceso debe tenerse en cuenta que cuando las personas afectadas son muy numerosas, esto puede comportar una serie de problemas para poder atender la sol solicitud de acceso con las debidas garantías, en concreto, otorgar el trámite de audiencia previsto en el artículo 31 de la LTC y valorar, caso por caso, si debe prevalecer la protección de datos personales o el derecho de acceso de la persona reclamante.

Una ponderación razonada entre los diferentes derechos e intereses en juego que debería realizarse de acuerdo con el artículo 24.2 de la LTC, obligaría a tener en cuenta esta circunstancia que puede comportar una denegación del acceso a esta información en caso de no quedar suficientemente acreditada la relevancia que pueda tener para la persona solicitante disponer de esa información.

Si bien no es obligatorio incluir en la solicitud los motivos por los que se pide el acceso (artículos 18.2 y 26.2 LTC), de no hacerlo, este elemento no se puede tener en cuenta a la hora de valorar los diferentes derechos e intereses en juego. Así, si no se aduce ningún motivo concreto, el acceso debería entenderse enmarcado dentro de la finalidad de la propia ley de transparencia (artículo 1.2 LTC).

Por todo ello, a todos los efectos, no aparecería como justificado, desde el punto de vista de la protección de datos, la obtención de manera generalizada por una persona ex trabajadora de una copia del conjunto de correos electrónicos profesionales. Esto, sin perjuicio de que en algún caso concreto pudiera resultar justificado el acceso y la obtención de copia de determinados correos electrónicos en atención a las circunstancias o motivos concretos que pudiera alegar (por ejemplo, en caso de tratarse de información necesaria para su derecho de defensa).

A todo ello, destacar que la LTC no establece plazo alguno en cuanto a la conservación de la información y documentación pública, a efectos de garantizar el ejercicio del derecho de acceso (artículo 18 LTC). Por tanto, no es obligatorio conservar la información de que se dispone para atender eventuales peticiones de acceso, más allá de los plazos de conservación previstos en las disposiciones que resulten de aplicación al caso concreto.

En este caso, como se ha visto, el cese de la relación laboral comportará la supresión de la cuenta de correo electrónico corporativa de la persona trabajadora, lo que dará lugar a su bloqueo, en los términos del artículo 32 del LOPDDDD y con las particularidades señaladas en el fundamento jurídico VII.

Tal y como ha puesto de manifiesto esta Autoridad en el informe IAI 6/2022 (disponible en la web), el bloqueo de información personal no debería vaciar de contenido la posibilidad de ejercer otros derechos, como el derecho de acceso información pública, en los términos de la legislación de transparencia.

La comunicación de datos bloqueados en este caso tendría por finalidad cumplir con una obligación del responsable, fundamentada en la Constitución (art. 105.b) CE) y en la LTC, por lo que, como se puso de manifiesto en el dictamen CNS 76/2016 (disponible en la web), podría resultar lícita sobre la base jurídica del artículo 6.1.c) del RGPD.

Cumplido el plazo de bloqueo de la información que proceda, deberá procederse a la eliminación efectiva de los correos electrónicos.

Por tanto, hacer notar que la atención de un eventual derecho de acceso (y obtención de copia) de una persona ex trabajadora en relación con los correos electrónicos puede llevarse a cabo mientras el Ayuntamiento disponga de esta información pública.

Conclusiones

La política de uso de los sistemas de información y dispositivos digitales que está elaborando el Ayuntamiento debe abarcar normas claras sobre la gestión que se hará de la cuenta de correo electrónico corporativa personalizada, y sobre los accesos a la información que contiene, tanto con motivo de cese de la relación laboral como en caso de ausencia temporal de la persona trabajadora, teniendo en cuenta las consideraciones hechas en los apartados III a VIII de este dictamen.

También debe incluir previsiones específicas respecto al uso adecuado de los sistemas de información por parte de su personal y el control que puede realizar el Ayuntamiento para garantizar su seguridad y buen funcionamiento.

Respecto a las peticiones de acceso y obtención de copia de los correos electrónicos por parte de personas ex trabajadoras, se tendrán en cuenta las observaciones realizadas en el apartado X de este dictamen.

Barcelona, 12 de diciembre 2022