

Identificación del expediente

Resolución de archivo de la información previa núm. IP 474/2021, referente al Ayuntamiento de El Prat de Llobregat

Antecedentes

1. En fecha 19/11/2021, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito formulado por dos personas en representación de la sección sindical SPL-CME El Prat de Llobregat, por el que denunciaban al Ayuntamiento de El Prat de Llobregat, con motivo de un presunto incumplimiento de la normativa de protección de datos personales.

En concreto, el sindicato denunciante ponía de manifiesto que, los días 15/09/2021, 16/09/2021 y 17/09/2021, varios agentes de la Policía Local del Ayuntamiento de El Prat de Llobregat habrían recibido en las suyas direcciones de correo electrónico corporativas, un correo enviado desde la dirección <(...)@gmx.com> cuyo asunto se refería a “*Reflexionemos sobre el SPL-CME*”, mediante el cual se criticaba el “comportamiento sindical” de las personas representantes del Sindicato SPL-CME El Prat de Llobregat (el aquí denunciante). A continuación, señalaba que el envío del correo electrónico a las referidas personas trabajadoras, se llevó a cabo sin utilizar la opción de la copia oculta, al tiempo que mostraba su preocupación por que personas ajenas al Ayuntamiento (en concreto, el titular de la cuenta <(...)@gmx.com> hubiesen podido acceder a las direcciones electrónicas corporativas de algunos agentes del cuerpo de la Policía Local.

Asimismo, el sindicato denunciante explicaba que, ante el envío de estos correos electrónicos a las direcciones corporativas de miembros del cuerpo de la Policía Local -lo que consideraba “un ataque *informático*”-, contactó telefónicamente y también mediante correo electrónico - enviado desde la dirección corporativa del sindicato-, con la unidad de Sistemas y Tecnologías de la Información y las Comunicaciones del Ayuntamiento (en adelante, SITIC), poniendo en su conocimiento estos hechos; y que, en respuesta a este correo electrónico, en fecha 18/10/2021 el SITIC les envió un correo electrónico informando sobre cómo deberían actuar las personas trabajadoras ante un correo presuntamente malicioso, y comunicándoles que el incidente referente a el envío de correos electrónicos desde la dirección <(...)@gmx.com> “*no tuvo más trascendencia que la molestia de los usuarios que lo recibieron, pero eso es inevitable, son direcciones de correo de una entidad pública y, por tanto, mucho más expuestas al dominio público*”.

Por último, el sindicato aquí denunciante exponía que, tras recibir este correo del SITIC, constataron que los correos electrónicos que habían recibido desde la dirección <(...)@gmx.com> habían desaparecido tanto de la cuenta de correo electrónico corporativo del sindicato, como de los correos electrónicos de los agentes que lo recibieron. Ante este hecho, el aquí denunciante manifestaba que no entendían “*cómo han podido acceder tanto a la cuenta del sindicato como a las cuentas de los agentes y hacer limpieza, ya que cada una tiene su propia contraseña*”

El escrito de denuncia se acompaña, entre otra documentación, de la copia del correo electrónico recibido desde la dirección <(...)@gmx.com>, en la que se constata que únicamente se remitió a determinadas direcciones de correo electrónico corporativas de personal del Ayuntamiento.

2. La Autoridad abrió una fase de información previa (núm. IP 474/2021), de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles motivar la incoación de un procedimiento sancionador.

3. En esta fase de información, en fecha 13/07/2022 se requirió la entidad denunciada para que informara sobre si el Ayuntamiento o alguna persona vinculada al mismo, envió el controvertido correo electrónico a determinados agentes del cuerpo de la Policía Local, desde la dirección <(...)@gmx.com>. Asimismo, también se requería al Ayuntamiento para que confirmara si gestiona las cuentas de correo electrónico de su personal y si, como gestor o administrador de estas cuentas, accedió a los buzones de los trabajadores procediendo a la supresión del correo electrónico de referencia .

4. En fecha 18/07/2022, la entidad denunciada respondió a dicho requerimiento a través de un escrito en el que, en síntesis, exponía lo siguiente (el subrayado es nuestro):

- *El lunes 20/09/2021 13:20 la técnica [...] del servicio de Sistemas y Tecnologías de la Información y las Comunicaciones (SITIC) solicita al servicio de oficina técnica especializada, que ofrece el apoyo y asesoramiento en temas transversales de seguridad al servicio, la verificación de dos correos recibidos, que presentan el perfil de correo peligroso o no deseable (SPAM), entre los que se encuentra el correo enviado a los agentes de la policía local, cuyos títulos son los siguientes: "EQUIPO DE VERIFICACIÓN MICROSOFT !!!" y "Reenviar: Reflexionamos sobre el SPL-CME". El procedimiento en estos casos es el siguiente: 1. Se analizan los correos para comprobar si son correos potencialmente peligrosos o no deseados (SPAM). 2. Si el resultado es positivo se procede a su eliminación de forma automatizada de los sistemas informáticos del Ayuntamiento, con el objetivo de evitar cualquier riesgo que pudiera derivarse. 3. Se bloquean las direcciones de origen para evitar la recepción futura de estas direcciones. En ambos casos se detectaron correos no deseables o SPAM, procediendo a aplicar el protocolo. Ésta es una tarea muy habitual y ordinaria para los servicios de tecnología y seguridad de toda organización, los ataques informáticos son un gran riesgo que compromete de forma constante y global la seguridad de los sistemas informáticos."*

Al respecto, el Ayuntamiento informaba que la cuenta <(...)@gmx.com> es ajena y externa a la corporación, y que el envío del referido correo electrónico no se trató de una intrusión a los sistemas de el Ayuntamiento, sino que se trataba de un correo de tipología no deseada. Al respecto, añadía que, en cuanto el SITIC tuvo conocimiento de la recepción de este mensaje, "se procedió a aplicar el protocolo de correos maliciosos y anti -SPAM, y se procedió a la purga del correo así como al bloqueo de los remitentes, derivado de la propia petición formulada por el Sindicato SPL-CME".

En último término, la entidad imputada señalaba que desde el SITIC no se puede conocer quién envió el correo originario, al tratarse de una cuenta ajena y externa al Ayuntamiento.

5. En fecha 25/08/2022, también en el seno de esta fase de información previa, se requirió de nuevo al Ayuntamiento para que, entre otros, confirmara si gestiona las cuentas de

correo electrónico de su personal y si, como a gestor o administrador de estas cuentas, accedió procediendo a la supresión del mensaje de referencia del buzón de entrada del correo electrónico de las personas destinatarias.

6. En fecha 28/08/2022 el Ayuntamiento dio respuesta al requerimiento de información señalado en el antecedente anterior, en los siguientes términos:

- “ *El Ayuntamiento no suministró los datos relativos a las direcciones de correo electrónico corporativas de determinadas personas trabajadoras a ninguna persona interna o externa de la organización (...)*”
- “ *El Ayuntamiento tiene la obligación de gestionar la seguridad de las cuentas de correo, por tanto dispone de un protocolo de eliminación masivo de correos sospechosos de spam o maliciosos. No se entra en ningún buzón personal, se eliminan de forma masiva cuando son detectados mediante las herramientas que ofrecen los propios sistemas a tales efectos* ”.

Fundamentos de derecho

1. De acuerdo con lo que prevén los artículos 90.1 de la LPAC y 2 del Decreto 278/1993, en relación con el artículo 5 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y el artículo 15 del Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, es competente para dictar esta resolución la directora de la Autoridad Catalana de Protección de Datos.

2. A partir del relato de antecedentes, es necesario analizar los hechos denunciados que son objeto de la presente resolución de archivo.

El sindicato denunciante se quejaba de que una tercera persona, titular de la cuenta <(...)@gmx.com> , habría dirigido un correo electrónico a las cuentas de correo electrónico corporativas de determinadas personas trabajadoras del Ayuntamiento, sin que éstas le hubiesen facilitado previamente sus direcciones y sin haber obtenido el consentimiento de estas personas, para llevar a cabo el envío del mensaje referido. Asimismo, el ahora denunciante también ponía de manifiesto que, después de informar al SITIC, una tercera persona –que no identifica– habría suprimido el mensaje controvertido de las cuentas de correo electrónico corporativo de las personas que le recibieron.

2.1 En relación con la presunta filtración de los datos relativos a las direcciones de correo electrónico corporativo

Como cuestión previa, procede analizar si las direcciones de correo electrónico corporativas del personal del Ayuntamiento encajan dentro de la definición de dato personal que, de acuerdo con el artículo 4.1 RGPD, es la siguiente: “ *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;*”

Al respecto, es preciso tener presente el dictamen CNS 4/2011 de esta Autoridad que recoge la siguiente argumentación:

“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 el que se gestione este dominio, sin que esto requiera un esfuerzo desproporcionado por parte de 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.”

De lo expuesto, no hay ninguna duda en atribuir a las direcciones de correo electrónico corporativo de las personas trabajadoras del Ayuntamiento la condición de dato personal, y por tanto su tratamiento debe estar sometido a los principios y garantías del 'RGPD.

Asentado lo anterior, y en cuanto a la eventual filtración de las direcciones corporativas denunciada, el Ayuntamiento ha afirmado no haber suministrado estos datos a terceras personas, y ha informado que el listado de personas trabajadoras, sus extensiones y sus correos electrónicos, se pueden consultar en el directorio de la Intranet del Ayuntamiento. En este sentido, la entidad denunciada ha alegado que " en el caso de la policía local se suelen hacer comunicaciones al grupo de agentes de forma ordinaria, por tanto es viable por cualquier persona interna obtener esta información", y ha informado que desconoce la identidad de la persona titular de la cuenta de correo electrónico <(...).@gmx.com>.

Al respecto, esta Autoridad no dispone de ningún indicio que permita sostener que el Ayuntamiento haya filtrado esta información a la persona titular de la cuenta de correo electrónico controvertida, ni que el Ayuntamiento tenga vinculación alguna con la titularidad de la cuenta <(...).@gmx.com>.

En relación con lo anterior, debe tenerse en cuenta que, aparte de las personas trabajadoras del Ayuntamiento que, obviamente, pueden tener acceso a dichas direcciones corporativas, no se puede descartar que terceras personas hayan obtenido esta información por sus propios medios – a título de ejemplo, personas que hayan prestado servicios en el Ayuntamiento, ciudadanos o ciudadanas que se hayan relacionado con estos empleados públicos, entre otros-, especialmente, atendiendo a que el mensaje fue recibido por algunos agentes de la Policía Local, pero no todos.

Así las cosas, esta Autoridad no puede atribuir al Ayuntamiento ni el envío del referido mensaje, ni la revelación o filtración al titular de la cuenta de correo electrónico <(...).@gmx.com> de la información relativa a las direcciones de correo corporativo de determinadas personas trabajadoras de la corporación.

2.2 En relación con la supresión de los correos electrónicos

En cuanto a la supresión del mensaje enviado desde la dirección <(...)@gmx.com> el sindicato denunciante exponía que “ *no entendemos cómo han podido acceder tanto a la cuenta del sindicato como a las cuentas de los agentes y hacer limpieza, puesto que cada uno tiene su propia contraseña*”.

A su vez, la entidad denunciada, consultada por esta Autoridad, ha reconocido haber suprimido del buzón de entrada de determinadas direcciones corporativas, correspondientes a agentes del cuerpo de la Policía Local y al sindicato denunciante, el correo electrónico enviado desde el dirección <(...)@gmx.com> dado su carácter de correo no deseado.

Además, el Ayuntamiento ha informado haber aplicado el Protocolo que utiliza en caso de detectar correos no deseados, que consiste en la eliminación, por medio de un sistema automatizado, del mensaje de referencia, sin que sea necesario que ninguna persona entre en los buzones de correo electrónico de las personas destinatarias del mensaje.

Por tanto, de acuerdo con lo expuesto, dado que el Ayuntamiento ha confirmado haber suprimido el mensaje de referencia, por medios automatizados, sin haber entrado en la cuenta de las personas que lo recibieron -actuación que técnicamente es del todo viable-, y dado que esta Autoridad no dispone de elementos que permitan sostener lo contrario, cabe concluir que la actuación de la entidad denunciada no contravino la normativa de protección de datos.

3. De conformidad con todo lo expuesto en el fundamento de derecho 2º, y dado que durante las actuaciones llevadas a cabo en el marco de la información previa no se ha acreditado, en relación con los hechos que se han abordado en la misma resolución, ningún hecho que pueda ser constitutivo de alguna de las infracciones previstas en la legislación sobre protección de datos, procede acordar su archivo.

El artículo 10.2 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, prevé que “(...) no se formulará pliego de cargos y se ordenará el sobreseimiento del expediente y el archivo de las actuaciones cuando de las diligencias y de las pruebas practicadas, resulte acreditada la inexistencia de infracción o responsabilidad. Esta resolución se notificará a los interesados”. Y el artículo 20.1) del mismo Decreto determina que procede el sobreseimiento: a) *Cuando los hechos no son constitutivos de infracción administrativa;* b) *Cuando no existen indicios racionales de haberse producido los hechos que han sido la causa de la iniciación del procedimiento (...)*”

Por tanto, resuelvo:

- 1.** Archivar las actuaciones de información previa número IP 474/2021, relativas al Ayuntamiento de El Prat de Llobregat.
- 2.** Notificar esta resolución al Ayuntamiento de El Prat de Llobregat ya la persona denunciante.
- 3.** Ordenar la publicación de la resolución en la web de la Autoridad (apdcat.gencat.cat), de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre.

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con el artículo 14.3 del Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, las personas interesadas pueden interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevé el artículo 123 y siguientes de la Ley 39/2015. También se puede interponer directamente un recurso contencioso administrativo ante los juzgados de lo contencioso administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Asimismo, las personas interesadas pueden interponer cualquier otro recurso que considere conveniente para defender sus intereses.

La directora,

Traducción automática