Calle Rosselló, 214, esc. A,1º 1a
08008 Barcelona

En esta resolución se han ocultado las menciones a la población afectada para dar cumplimiento al arte. 17.2 de la Ley 32/2010, dado que, en caso de revelar el nombre de la población afectada, podrían identificarse también las personas físicas afectadas.

Identificación del expediente

Resolución de archivo de la información previa núm. IP 73/2021, referente al Ayuntamiento de (...).

Antecedentes

1. En fecha 18/02/2021, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de una persona por el que formulaba una denuncia contra el Ayuntamiento de (...), con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales, y en el mismo escrito también denunciaba una denuncia contra una determinada actuación de el Área Básica Policial de (...)(en adelante, ABP) en respuesta a una petición de un Juzgado.

En concreto, y en cuanto al Ayuntamiento de (...), la persona denunciante exponía lo siguiente:

1.1. Que en fecha (...)el inspector jefe de la Guardia Urbana de (...) envió un correo electrónico al jefe del Área de Seguridad en Tecnologías de la Información de la División de Sistemas de Información Policial (en adelante, DSIP) de la Dirección General de la Policía (DGP) del Departamento de Interior, mediante el cual solicitó que se diera de baja como usuaria del SIP a la persona aquí denunciante. Como motivos de queja, la persona denunciante exponía, por un lado, que ese correo electrónico no se había enviado de forma cifrada, tal y como establece el Manual de Seguridad del SIP; y por otra parte, que el correo se había enviado al jefe de la DSIP, cuando el citado Manual de Seguridad señala que estos correos de solicitud de baja de usuario no deben enviarse a dicho jefe.

1.2. La persona denunciante exponía, de forma inconcreta, que se habían solicitado auditorías "sin datos objetivos" a una persona que no era la responsable, refiriéndose al jefe del ABP de (...). La persona denunciante no aportaba ningún documento a efectos de acreditar estos hechos denunciados.

1.3. Por último, solicitaba el acceso a diversa información.

La persona denunciante aportaba copia de un oficio emitido en fecha 07/08/2020 por el jefe del ABP mencionado, dirigido a dicho Juzgado de Primera Instancia e Instrucción (...)de (...), en el que se exponía lo siguiente:

> "En respuesta a su oficio (...) le informamos que, según la Unidad de Auditorías de la División de Sistemas de Información policial consta que:

Calle Rosselló, 214, esc. A,1º 1a
08008 Barcelona

> En fecha (...), el Inspector Jefe de la Guardia Urbana de (...), SR. (...) -nombre y apellidos solicitó, vía correo electrónico dirigido al jefe del Área de Seguridad en Tecnologías de la Información de la División de sistemas de Información Policial, que con carácter de urgencia se bloqueara inmediatamente el acceso al SIP del usuario (...)
> -nombre y apellidos de la persona denunciante- puesto que se le había abierto expediente disciplinario por Decreto de alcaldía núm. (...), de fecha (...)."

2. En relación con los hechos denunciados relativos a la actuación del Ayuntamiento de (...) la Autoridad abrió la presente fase de información previa (núm. IP 73/2021), 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 de motivar la incoación de un procedimiento sancionador.

Por lo que se refiere a los hechos denunciados relativos a la actuación de una ABP de la Policía de la Generalidad Mossos d'Esquadra, adscrita a la DGP del Departamento de Interior, la Autoridad abrió la fase de información previa núm. IP 73bis/2021.

En la presente resolución, se abordan los motivos de denuncia referidos a la actuación del Ayuntamiento de (...) descritos en los antecedentes.

3. En fecha 26/02/2021, la Autoridad requirió a la entidad denunciada para que concretara si el correo controvertido del inspector jefe de la Guardia Urbana (GU) de (...) (antecedente 1, apartado 1.1 .), se había enviado de forma cifrada.

4. En fecha 15/03/2021, el Ayuntamiento de (...) respondió el requerimiento mencionado a través de un escrito en el que exponía lo siguiente:

> "El Ayuntamiento de (...), trabaja en la aplicación y cumplimiento de medidas de seguridad suficientes y necesarias de acuerdo con la normativa aplicable y riesgos detectados.
>
> Que en el marco de esta información previa, el correo electrónico que se envió al jefe del Área de Seguridad en Tecnologías de la Información estaba en relación a una petición de baja de un usuario de la aplicación SIP de Policía Local .
>
> Que el Manual de altas, bajas y modificaciones de usuarios de las policías locales en los SIP de la DGP se establece: Cualquier petición enviada por un buzón no autorizado, mal rellenado o sin encriptar será denegada.
>
> Que el Ayuntamiento de (...) no tiene conocimiento ni ha podido contrastar si el correo electrónico en cuestión se envió encriptado pues no está previsto el acceso a correos electrónicos de

Calle Rosselló, 214, esc. A,1º 1a
08008 Barcelona

trabajadores a excepción de casos excepcionales en el marco de sospechas de vulneración de protocolos y normativas."

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, se deben analizar los hechos denunciados que son objeto de la presente resolución de archivo.

2.1. Sobre la encriptación del correo a través del cual se solicitó la baja de usuario del SIP, y sobre la persona a la que se envió dicho correo.

En primer lugar, la persona denunciante exponía que en fecha (...)el inspector jefe de la Guardia Urbana de (...) envió un correo electrónico sin cifrar al jefe de la DSIP, a fin de que lo diera de baja como usuario del SIP, contraviniendo lo previsto en el Manual de Seguridad del SIP (antecedente 1).

El citado Manual de Seguridad figura incorporado como anexo 2 al convenio sobre las conexiones a los Sistemas de Información Policial suscrito entre la DGP y el Ayuntamiento de (...)
(que fue aportado junto con la denuncia que dio lugar al procedimiento sancionador núm. PS 45/2019).
El apartado 2.2 de este Manual, viene referido a las comunicaciones efectuadas entre la persona interlocutora informática en el ámbito de las Policías Locales conectadas al SIP y el responsable de seguridad de los SIP, y ciertamente de su lectura se desprende la obligatoriedad de cifrar o encriptar los mensajes de correo electrónico que contengan solicitudes de baja de usuarios del SIP, como sigue:

> "(...) El envío de información confidencial a través del correo electrónico tal y como lo son los códigos de usuario y las claves de paso para acceder a los SIP, los nombres y apellidos de los titulares de los códigos, así como otro tipo de información relacionada con estos sistemas deberá hacerse obligatoriamente mediante la encriptación de los mensajes de correo electrónico y sus documentos anejos."

Por otra parte, en el mismo apartado del Manual de Seguridad se indica la siguiente dirección electrónica del servicio de atención al usuario de la DGP (Help Desk) a donde dirigir, entre otras, las solicitudes de baja de usuarios:

- (...): destinada a las comunicaciones de altas y bajas de usuarios, incidencias, consultas, etc.

Calle Rosselló, 214, esc. A,1º 1a
08008 Barcelona

ya continuación se señala lo siguiente:

> "el envío de mensajes se hará a alguna de estas direcciones - entre la que figura la indicada antes- según cuál sea el caso y se evitará el envío a las direcciones directas de los responsables de la DSIP para los supuestos aquí descritos."

A partir de este contenido del Manual de Seguridad, la persona denunciante considera que el jefe de la GU de (...) contravino este Manual de Seguridad por haber enviado el correo electrónico al jefe de la DSIP (en lugar de enviarlo a la dirección electrónica que se indicaba en el Manual), así como por haberlo enviado sin encriptar. Con esta queja, el denunciante se refiere a la posible vulneración del deber de confidencialidad y de una medida de seguridad.

En este sentido, el artículo 5.f) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de éstas (RGPD), prevé que los datos personales deben tratarse de forma que se garantice una seguridad adecuada, mediante la aplicación de medidas técnicas u organizativas adecuadas. A continuación se analizarán separadamente los dos motivos de denuncia referidos al envío del mismo correo.

2.1.1. En primer lugar, en cuanto al envío del correo electrónico al jefe de la DSIP, extremo que el Ayuntamiento ha confirmado, debe constatarse de entrada que de la lectura del apartado 2.2. del Manual de Seguridad del SIP ("...se evitará el envío a las direcciones directas de los responsables"), no se desprende con claridad que no se pueda enviar este tipo de correos al jefe de la DSIP, en el sentido de norma de prohibición, sino que esta disposición podría obedecer a razones operativas o de organización del servicio, en el sentido de considerar que el envío de las solicitudes de altas y bajas de usuarios del SIP a unas direcciones concretas, permite gestionar mejor estas peticiones. En la interpretación de este apartado 2.2 del Manual de Seguridad, se tiene en cuenta el hecho de que el jefe de la DSIP al que se envió el correo, es el máximo responsable de la unidad encargada de la gestión del sistema de información policial (Decreto 415/2011, de 13 de diciembre, de estructura de la función policial de la Dirección General de la Policía). De modo que podría acceder a las solicitudes de baja de usuarios del SIP en ejercicio o para el cumplimiento de las funciones encomendadas.

Por otra parte, cabe constatar que la cláusula 5.7 del citado convenio suscrito entre la DGP y el Ayuntamiento de (...), podría amparar que el correo se hubiera enviado al jefe de la DSIP. Esta cláusula 5.7 lleva por título "interlocutor informático en el ámbito local y usuarios", y señala que el interlocutor "debe ser el Jefe de la Policía Local u otro policía local que éste designe", y que este interlocutor "ha de enviar al jefe del Área de Seguridad en

Calle Rosselló, 214, esc. A,1º 1a
08008 Barcelona

Tecnologías de la Información" determinada información, entre la que figura, por lo que aquí interesa, la siguiente:

- "Comunicar de forma inmediata todos los cambios que haya sobre los usuarios, debe solicitar las altas de usuarios y las bajas cuando algún usuario deje de pertenecer o prestar servicios, por cualquier motivo, a la Policía Local.

- Comunicar de forma inmediata cualquier incidencia, es decir, cualquier anomalía que afecte o pueda afectar a la seguridad de los datos del SIP, de acuerdo con lo que se establece en el Manual de Seguridad."

El presente caso, podría tener encaje en los supuestos transcritos, puesto que la solicitud de baja de usuario de la persona denunciante, obedecía a que el Ayuntamiento le había incoado un procedimiento disciplinario por presuntos accesos ilícitos al SIP, y se había adoptado una medida cautelar. Es decir, que con el correo que envió el inspector jefe de la GU de (...) al jefe de la DSIP, le comunicaba la incidencia que afectaba a la seguridad de los datos del SIP, y vinculada a ésta, formulaba con carácter de urgencia la solicitud de baja como usuario del SIP a la persona que presuntamente había accedido ilícitamente al SIP. En tal caso, el envío del correo por parte del jefe de la GU al jefe de la DSIP, se fundamentaría en el cumplimiento de una obligación legal de acuerdo con los artículos 6.1.c) y 5.1.f) del RGPD, así como en el cumplimiento de una misión realizada en interés público o el ejercicio de poderes públicos de conformidad con el artículo 6.1.e) del RGPD y la Ley 16/1991.

De acuerdo con las razones apuntadas, no se observa con la claridad necesaria que el hecho de haber enviado un correo electrónico al jefe de la DSIP, sea constitutivo de infracción. Pero incluso en su caso, se considera que estos hechos no revisten entidad suficiente para incoar un procedimiento disciplinario, dadas las circunstancias señaladas.

2.1.2. En segundo lugar, en cuanto al envío del correo electrónico sin cifrar, el Ayuntamiento de (...) ha manifestado, mediante escrito de fecha 15/03/2021, que "no tiene conocimiento ni ha podido contrastar si el correo electrónico en cuestión se envió encriptado". Y en su respuesta también se ha referido al punto del Manual de Seguridad donde se señala que: "cualquier petición enviada por un buzón no autorizado, mal rellenado o sin encriptar será denegada", dando a entender que si el Ayuntamiento hubiera enviado el correo sin cifrar, la solicitud de baja de usuario habría sido denegada, lo que no sucedió, puesto que la DSIP dio de baja del SIP a la persona denunciante.

Así las cosas, las manifestaciones efectuadas por la persona denunciante, sin aportar ningún elemento probatorio que las fundamente -aunque sea de forma indiciaria-, parecen meras sospechas, las cuales por sí mismas no permiten inferir que el Ayuntamiento podría haber cometido la infracción apuntada, y en consecuencia iniciar un procedimiento sancionador.

Calle Rosselló, 214, esc. A,1º 1a
08008 Barcelona

Pero incluso si fuera el caso, no procedería iniciar la acción impugnatoria debido a que la eventual infracción cometida estaría prescrita, dado que el correo electrónico en cuestión se envió el día 04/03/2019.

En efecto, el artículo 83.4.a) del RGPD tipifica como infracción la vulneración de las obligaciones del responsable previstas en varios preceptos del RGPD, entre los que figura el cifrado de datos personales (art. 32.1.a RGPD ). Por su parte, el artículo 73 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD), ha recogido como infracción grave el incumplimiento de las medidas de seguridad implementadas (art. 73.g).

El artículo 73 de la LOPDDDD prevé que las infracciones graves prescriben a los dos años. Pues bien, en el momento de dictarse la presente resolución, este plazo de prescripción se habría superado. En esta valoración del cómputo del plazo, se ha tenido en cuenta el período de suspensión del plazo previsto en la disposición adicional 4ª del Real Decreto 463/2020 de 14 de marzo, por el que se declaró el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por la COVID-19. Por consiguiente, en el negado supuesto que se considerase que los hechos denunciados son constitutivos de infracción, ésta habría prescrito, lo que provoca la extinción de la responsabilidad de la eventual conducta infractora.

2.2. Sobre las peticiones de auditorías formuladas sin causa legal y dirigidas a incompetente persona.

A continuación, la persona denunciante exponía, de forma inconcreta, que se habían solicitado auditorías “sin datos objetivos” a una persona que no era la responsable, y refiriéndose al jefe del ABP de (...) , como sigue: “que la petición de auditorías...no se ajustan a la legalidad en cuanto a que sin datos objetivos se pide una auditoría a quien no es responsable (Ninguno del ABP de (...) ) para intentar encontrar un hecho que lleve a pedir otra auditoría (...)”.

Sin embargo, lo cierto es que la persona denunciante no concretaba a qué auditorías se refería, ni aportaba ningún documento a efectos de acreditar estos hechos que denunciaba, ni mencionaba la norma que a su juicio se habría contravenido.

Pese a esta inconcreción, todo parece indicar que la persona denunciante podría referirse a una solicitud de auditoría que formuló el jefe de la GU de (...) en fecha 12/12/2018.

Al respecto de esta solicitud de auditoría, la persona denunciante ya formuló ante la Autoridad una denuncia anterior (que dio lugar a la apertura de la IP 342/20), mediante la cual exponía que esta solicitud de auditoría era ilegal, puesto que no se atendía a derecho ni el motivo real para pedirla, ni la finalidad perseguida. En ese caso, tras las oportunas actuaciones de investigación, la Autoridad dictó una resolución de archivo, de fecha

Calle Rosselló, 214, esc. A,1º 1a
08008 Barcelona

18/10/2021, por considerar que tanto la petición de la auditoría como su realización eran legítimas, como sigue (fundamento de derecho 2.1:

> "(...) la petición de dicha auditoría por parte del jefe de la GU se fundamentaba en el cumplimiento de una obligación legal de acuerdo con los artículos 6.1.c), 5.1.f) y 32 del RGPD , así como en el cumplimiento de una misión realizada en interés público o el ejercicio de poderes públicos de conformidad con el artículo 6.1.e) del RGPD y la Ley 16/1991.
>
> A su vez, la realización de la auditoría por parte de la DSIP (DGP) también se sustentaría en las mismas bases jurídicas. Por tanto, estos tratamientos son lícitos.
>
> Así pues, con independencia del contenido de la solicitud que formuló el jefe de la GU (quien debe considerarse que es una persona autorizada para solicitar una auditoría sobre los accesos al SIP) en fecha 12/12/2018 (la cual el denunciante no aporta), a quien le corresponde la decisión final de elaborar una auditoría es al responsable del tratamiento, es decir, a la DSIP.
>
> En cualquier caso, se debe reiterar que esta auditoría debe entenderse que es una medida de seguridad que permite verificar cualquier consulta que se haya efectuado en el SIP y en cualquier momento; así como que la finalidad perseguida es garantizar la seguridad de los datos incluidos en dicho sistema de información."

Así las cosas, con respecto a estos hechos denunciados, cabe concluir que la persona denunciante no ha aportado elementos que acrediten los hechos que denuncia, ni, en consecuencia, elementos de los que se infiera que el Ayuntamiento de (...) podría haber cometido una infracción. Y en todo caso, en cuanto a la solicitud de auditoría que el jefe de la GU de (...)
formuló en fecha 12/12/2018, y en la misma auditoría, la Autoridad ya se pronunció sobre la legitimidad de dichos tratamientos de datos.

2.3. Sobre otras cuestiones planteadas por la persona denunciante.

Por último, la persona denunciante solicitaba conocer determinada información, como sigue: "solicito conocer desde qué correo electrónico se hizo la petición ya qué correo electrónico se hizo, a fin de confirmar si se va ajustar a derecho y al protocolo mencionado (...) Que se me informe con claridad de las veces que se han auditado mis consultas en el aplicativo SIP, así como saber los motivos que la propiciaron".
Al respecto, es suficiente señalar que con estas manifestaciones, la persona denunciante no denuncia ninguna conducta contraria a la normativa sobre protección de datos, sino que pide determinada información, que no corresponde a esta Autoridad facilitar.

Calle Rosselló, 214, esc. A,1º 1a
08008 Barcelona

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 esta resolución, ningún hecho que pueda ser constitutivo de alguna de las infracciones previstas en la legislación sobre protección de datos, o en todo caso éstas hubieran prescrito, procede acordar su archivo.

El artículo 89 de la LPAC, en consonancia con los artículos 10.2 y 20.1 del Decreto 278/1993, prevé que procede archivar las actuaciones cuando en la instrucción del procedimiento se pone de manifiesto lo siguiente "a) La inexistencia de los hechos que puedan constituir la infracción; b) Cuando los hechos no estén acreditados; c) Cuando los hechos probados no constituyan, de forma manifiesta, una infracción administrativa"; e) Cuando se concluya, en cualquier momento, que la infracción ha prescrito".

Por tanto, resuelvo:

1. Archivar las actuaciones de información previa número IP 73/2021, relativas al Ayuntamiento de (...).

2. Notificar esta resolución al Ayuntamiento de (...) 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,