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 342/2020, referente al Ayuntamiento de (...).

Antecedentes

1. En fecha 13/11/2020, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de una persona (agente de la Guardia Urbana de (...) -en adelante, GU-) por el que formulaba una denuncia contra el Ayuntamiento de (...), con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales.

En primer lugar, la persona denunciante exponía que en fecha 12/12/2018, el jefe de la GU pidió a la División de los Sistemas de Información Policial (en adelante, DSIP) de la Dirección General de la Policía (en adelante, DGP) del Departamento de Interior, una auditoría de los accesos a los sistemas de información policial (en adelante, SIP) sin cumplir con los requisitos legales mínimos (según la persona denunciante: motivación real para pedirla, finalidad perseguida y motivación de la concreción del período a auditar).

Añadía la persona denunciante que, según se indica en el informe que elaboró el jefe de la GU se verificaron 12.500 consultas en el SIP, pero en el informe sólo se hacía referencia a unas 40 consultas (el 0,2% del total).

La persona denunciante también solicitaba saber por qué conducto se hicieron llegar los datos auditados y quién los recibió y dónde; qué se ha hecho con el resto de datos; así como por qué han sido desestimadas y bajo qué criterio.

2. La Autoridad abrió una fase de información previa (núm. IP 342/2020), 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.

3. En el marco de esta fase de información previa y de la iniciada a raíz de la denuncia de otra persona contra el Ayuntamiento de (...) (IP 333/2020) relacionada con los mismos hechos, en fecha 03 / 03/2021 se requirió dicha entidad para que aportara el análisis de riesgos para determinar las medidas para garantizar la seguridad en los sistemas del Ayuntamiento de los datos consultados en el SIP; así como si la información vinculada a las consultas que no se

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

consideraron ilícitas (es decir, las que no fueron objeto de los expedientes disciplinarios), había sido suprimida o bloqueada.

4. En fecha 08/04/2021, el Ayuntamiento de (...) respondió el requerimiento mencionado a través de un escrito en el que exponía, entre otros, lo siguiente:

- Que consultada la GU y los departamentos del Ayuntamiento que pudieran tener constancia de la demanda de un análisis de riesgos en relación con las consultas efectuadas en el SIP, se desconoce de la existencia del mismo.
- Que consultados los servicios implicados, no constaba que ningún dato hubiera sido suprimido o bloqueada de ningún registro ni municipal, ni supramunicipales en relación con consultas efectuadas.

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 los requisitos de la auditoría.

La persona denunciante exponía que, en fecha 12/12/2018, el jefe de la GU pidió a la DSIP una auditoría de los accesos al SIP (realizados por él y otro agente de la GU) sin cumplir con los requisitos legales mínimos, que según la persona denunciante serían la motivación real para pedirla, la finalidad perseguida y la motivación de la concreción del período a auditar.

Cabe remarcar que la persona denunciante ni aportaba la solicitud de auditoría que habría formulado el jefe de la GU en fecha 12/12/2018; ni tampoco concretaba la norma que recogería dichos requisitos legales que, según el denunciante, deberían cumplir las solicitudes de auditoría.

Dicho esto, procede poner el énfasis en que la auditoría o el registro de accesos es una medida de seguridad destinada a verificar que los accesos al sistema de información se han realizado en el ejercicio de las funciones encomendadas a las personas usuarias que acceden.

El artículo 5.1.f) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27/4, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales y

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

en la libre circulación de éstas (en adelante, RGPD) contempla el principio de integridad que implica que los datos personales deben tratarse de forma que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidental de los datos, mediante las medidas técnicas u organizativas adecuadas.

Por su parte, el artículo 32.1.d) del RGPD prevé que el responsable del tratamiento debe implementar las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya un proceso para verificar , evaluar y valorar regularmente la eficacia de las medidas técnicas y organizativas establecidas para garantizar la seguridad del tratamiento. Y el apartado 4º del artículo 32 del RGPD también determina que el responsable debe adoptar medidas para garantizar que cualquier persona que actúa bajo su autoridad y que tiene acceso a datos personales sólo puede tratar estos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del derecho de la Unión o de los Estados miembros.

Dado que la DGP del Departamento de Interior es la responsable del SIP, corresponde a ésta (a través de la DSIP) realizar las auditorías sobre los accesos a este sistema de información policial.

Pues bien, 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 corresponde la decisión final de elaborar una auditoría es el responsable del tratamiento, es decir, en 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.

2.2. Sobre las 12.500 consultas auditadas.

La persona denunciante ponía de manifiesto que en el informe que elaboró el jefe de la GU (se infiere que se refiere al informe emitido el 01/02/2019) se pone de manifiesto que se

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

verificaron 12.500 consultas al SIP (efectuadas por el denunciante y otro agente), pero que el informe sólo recogía unas 40 (el 0,2% del total).

Pues bien, esta circunstancia es irrelevante, en la medida en que todos los accesos que efectúen las personas usuarias a un sistema de información pueden ser objeto de auditoría.
Más aún teniendo en cuenta la naturaleza del SIP.

No se observa ningún incumplimiento de la normativa de protección de datos, debido a que el citado informe no recogiera información relativa a las consultas al SIP auditadas y que no deberían considerarse ilícitas. De hecho, esto se ajustaría al principio de minimización de los datos (art. 5.1.c RGPD), conforme el cual los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con las finalidades para las que se tratan.

Dicho esto, aunque no se denunciaba expresamente, procede poner de manifiesto que a fecha de hoy la directora de la Autoridad ha acordado iniciar un procedimiento sancionador contra el Ayuntamiento de (...) por no acreditar haber efectuado un análisis riesgos para determinar las medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos personales que se tratan en el marco de los procedimientos disciplinarios, como los vinculadas a las 12.500 consultas en el SIP controvertidas.

Vinculado con ello, la persona denunciante solicitaba saber que se había realizado con el resto de datos (las consultas al SIP auditadas y que no se habrían considerado ilícitas).

Esta cuestión debe entenderse que se refiere a la conservación del resto de los datos vinculados a las consultas al SIP auditadas y que no habrían sido objeto del procedimiento disciplinario incoado a la persona aquí denunciante ya otro agente.

Al respecto, procede acudir al artículo 5.1.e) del RGPD regula el principio de limitación del plazo de conservación determinante que los datos personales deben mantenerse de forma que permitan identificar a los interesados durante un período no superior al necesario para las finalidades del tratamiento. Y añade que los datos personales se pueden conservar durante períodos más largos, siempre que se traten exclusivamente con fines de archivo en interés público, entre otros.

Pues bien, sin perjuicio de que dichas consultas al SIP pudieran seguir siendo necesarias para alcanzar la finalidad pretendida, se infiere que en el presente caso estos datos recogidos durante las actuaciones previas al inicio de los procedimientos disciplinarios deberían conservarse con fines de archivo en interés público.

Al respecto, cabe señalar que la tabla de evaluación y acceso documental con código 751, relativa a la serie documental “Expedientes disciplinarios muy graves en materia de personal” (en el presente caso, las infracciones se calificaron como muy graves), contempla la conservación permanente, lo que también afectaría a la información recopilada tanto en el

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

marco de los propios procedimientos disciplinarios, como en el seno de las actuaciones previas llevadas a cabo con anterioridad al inicio del procedimiento.

2.3. Sobre otras cuestiones planteadas por la persona denunciante.

Seguidamente, la persona denunciante solicitaba saber por qué conducto se hicieron llegar los datos auditados y quién los recibió y dónde.

La persona denunciante no denuncia ninguna conducta contraria a la normativa sobre protección de datos, sino que pedía determinada información, que no corresponde a esta Autoridad facilitar.

Sin perjuicio de lo anterior, la información que solicitaba la persona denunciante podría llegar a poner de manifiesto un eventual incumplimiento del artículo 32 del RGPD (referente a la seguridad de los datos), que en su caso podría llegar a ser constitutivo de la infracción prevista en el artículo 83.4.a) del RGPD, que tipifica como infracción la vulneración de las obligaciones del responsable previstas en varios preceptos del RGPD, entre ellos el artículo 32 de el 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 tanto la falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento (art. 73.f), como el incumplimiento de las medidas de seguridad implementadas (art. 73.g).

Asimismo, el artículo 73 de la LOPDDDD también prevé que las infracciones graves prescriben a los dos años. Teniendo en cuenta que la auditoría se solicitó el 12/12/2018, la eventual vulneración de la seguridad de los datos habría prescrito (el 11/12/2020), es decir, unos días después de presentar -se la denuncia (13/11/2020).

La prescripción de la infracción provoca la extinción de la responsabilidad que pudiera derivarse de la eventual conducta infractora, lo que a su vez impediría incoar el procedimiento sancionador correspondiente, al no poder ya ejercer ninguna acción de persecución de la supuesta infracción .

Por otro lado, la persona denunciante también solicitaba conocer el motivo por el que el resto de 12.500 consultas en el SIP auditadas fueron desestimadas (es decir, no imputadas en el marco de los expedientes disciplinarios incoados por el Ayuntamiento a la persona denunciante ya otro agente).

Tampoco corresponde a esta Autoridad resolver esta consulta de la persona denunciante. En cualquier caso, es lógico inferir que si no se incluyeron determinadas consultas en el SIP auditadas entre los hechos imputados a los dos agentes de la GU a los que se les va

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

incoar un expediente disciplinario, esto probablemente estaría motivado por el hecho de que el Ayuntamiento no tendría indicios por considerar que aquellas consultas fueran ilícitas.

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, 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: "c) Cuando los hechos probados no constituyan, de forma manifiesta, una infracción administrativa".

Por tanto, resuelvo:

1. Archivar las actuaciones de información previa número IP 342/2020, 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,