

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 procedimiento sancionador núm. PS 52/2021, referente al Ayuntamiento de (...).

Antecedentes

1. En fecha 03/11/2020, tuvieron entrada en la Autoridad Catalana de Protección de Datos dos escritos de una misma 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.

En concreto, la persona denunciante exponía, entre otros, lo siguiente:

- 1.1. Que en el informe emitido el 01/02/2019 por el inspector jefe de la Guardia Urbana de (...) -en adelante, GU- (por el que se ampliaba el informe emitido en fecha 27/12/2018 en el que se solicitaba iniciar unas diligencias de investigación a dos funcionarios de la GU por accesos presuntamente indebidos al Sistema de Información Policial (en adelante, SIP) constaban los datos personales que otro agente de la GU había consultado a través del SIP.
- 1.2. Que mientras estaba de baja, el inspector jefe de la GU accedió a una instancia que presentó (a finales de enero de 2019) el representante de un determinado partido político (Sr. (...)), tal y como se constata en el informe de 01/02/2019. Añade que el expediente disciplinario incoado por el Ayuntamiento se fundamenta en varios informes elaborados por el inspector jefe de la GU también elaborados cuando estaba de baja.
- 1.3. Que se comunicó a los representantes sindicales, la incoación de los expedientes disciplinarios incoados a la persona denunciante ya otro agente.
- 1.4. Que se informó a la Candidatura de Unidad Popular (en adelante, CUP) sobre la incoación de los expedientes disciplinarios (incoados por el Ayuntamiento a la persona denunciante ya otro agente de la GU); así como a las personas afectadas por las consultas en el SIP que motivaron la incoación de un expediente disciplinario (a la persona denunciante ya otro agente).
- 1.5. Que en el informe emitido por el inspector jefe de la GU en fecha 26/06/2019 (en relación a la posible práctica dilatoria de las personas expedientadas a fin de que caducaran los procedimientos disciplinarios), contiene información referente al otro agente de la GU al que también se le incoó un expediente disciplinario.
- 1.6. Que tal y como se desprende del informe de 01/02/2019 antes mencionado, se verificaron 12.500 consultas efectuadas a través del SIP (6.500 en relación a personas físicas y 6.000 en relación a vehículos), pero que en el marco de el expediente disciplinario incoado sólo se incorporaron una pequeña parte. La persona denunciante también cuestionaba

cómo se custodiaba la información referente a las consultas que no se habrían considerado ilícitas.

El denunciante aportaba diversa documentación relativa a los hechos denunciados.

A esta denuncia se le asignó el número IP 333/2020.

2. La Autoridad abrió una fase de información previa, 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 fecha 14/11/2020, la persona denunciante presentó un nuevo escrito de denuncia contra el Ayuntamiento de (...) en el que exponía lo siguiente:

3.1. Que el Ayuntamiento de (...) manipuló 12.500 fichas (consultas) del SIP (que habría efectuado la persona denunciante y otro agente), sin los mínimos requisitos de seguridad.

3.2. Que se han comunicado a partidos políticos (la CUP) ya las personas afectadas la incoación de los expedientes disciplinarios (hecho ya había denunciado, tal y como se ha recogido en el antecedente 1.4), tales como al sr. (...).

La persona denunciante aportaba diversa documentación.

A esta denuncia se le asignó el número IP 344/2020.

4. En esta fase de información, en fecha 09/12/2020 se requirió a la entidad denunciada para que informara, entre otros, sobre los motivos por los que se facilitó a la persona denunciante el informe de 01/02/2019, sin anonimizar los datos relativos a otro agente, ni tampoco los datos referentes a terceras personas vinculadas a los accesos al SIP que ese otro agente efectuó; si el inspector jefe de la GU estaba en situación baja laboral cuando accedió a la instancia que había presentado el sr. (...) ante el Ayuntamiento; si las personas a quienes el jefe de Negociado de Personal y Organización comunicó, mediante correo electrónico, la incoación de dos expedientes disciplinarios eran delegados de personal o miembros de la junta de personal; los motivos por los que se facilitó a la persona denunciante el informe de 26/06/2019, sin anonimizar la información referente al otro agente de la GU al que también se incoó un expediente disciplinario; y en relación a las 12.500 consultas en el SIP, efectuadas por los agentes expedientados, a las que se refiere el informe de 01/02/2019, se requirió que se aportara copia del análisis de riesgos utilizado para determinar las medidas para garantizar la seguridad de estos datos en los sistemas del Ayuntamiento.

5. En fecha 31/12/2020, el Ayuntamiento de (...) respondió el requerimiento mencionado a través de un escrito en el que exponía, entre otros, el siguiente

- Que el informe de 01/02/2019 sin anonimizar, lo facilitó el entonces jefe de Personal, que ya no trabaja en el Ayuntamiento
- Que se desconoce cuando el jefe de la GU accedió a la instancia presentada por el sr. (...). El jefe de la GU estuvo de baja del 13/12/2018 al 15/02/2019.
- Que la base jurídica para acceder a dicha instancia deriva del artículo 27 de la ley 16/1991, de 10 de julio, de las policías locales (en adelante, Ley 16/1991).
- Que en relación al correo electrónico a través del cual se habría comunicado la incoación de dos expedientes, el actual jefe de Personal en funciones no tiene acceso al correo (el Jefe de personal que envió el correo, ya no trabaja en el Ayuntamiento). Sólo se ha podido acceder a la captura pantalla facilitada por la APDCAT [que había facilitado la persona denunciante y en la que sólo se identificaban 2 de los 5 destinatarios], por lo que sólo se ha podido saber datos de dos personas, (...) y (...), las cuales eran miembros de la Junta de Personal.
- Que el informe de 26/06/2019, sin anonimizar, lo facilitó el entonces jefe de Personal que ya no trabaja en el Ayuntamiento.
- Que la única persona que podía pedir la auditoría de los accesos al SIP era el Jefe de la GU, que en el momento de responder al requerimiento estaba de baja.
- Que el equipo de personal y organización del Ayuntamiento y su jefe en funciones, no disponen de esta auditoría, debería pedirse al Jefe de la GU. Tampoco disponen del análisis de riesgos que pueda haberse efectuado.
- Que las personas autorizadas para acceder a esta documentación (la auditoría de los accesos al SIP) son el jefe de la GU, el concejal y el alcalde.
- Que en relación con las consultas al SIP, efectuadas por los agentes expedientados, se desconoce si fueron suprimidas o bloqueadas.

6. En fecha 15/01/2021, la persona denunciante presentó un nuevo escrito de denuncia, en el que exponía lo siguiente:

- 6.1. Que el jefe de la GU solicitó al Departamento de Interior una auditoría, aun no siendo el interlocutor informático, contraviniendo el Manual de Seguridad del convenio de conexión de las policías locales al SIP.
- 6.2. Que dicha petición, que incluiría, según la persona denunciante, "los códigos de usuario y las claves de paso para acceder a los SIP, los nombres y apellidos de los titulares de los códigos", se formuló por correo electrónico no encriptado (dedo manual prevé que la comunicación de los códigos de usuario, las claves de paso para acceder al SIP y los nombres y apellidos de los titulares de los códigos, debe realizarse obligatoriamente mediante la encriptación de los mensajes de correo electrónico y de sus anexos).

La persona denunciante aportaba copia del Manual de Seguridad del convenio de conexión de las policías locales a los SIP de la DGP. En este manual, se especifica que el "envío de información confidencial [a la DGP] a través del correo electrónico tal 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 realizarse obligatoriamente mediante la encriptación de los mensajes de correo electrónico y sus documentos anexos.”

A esta denuncia se le asignó el número IP 18/2021.

7. En fecha 03/03/2021, se requirió nuevamente al Ayuntamiento de (...) para que, en caso de que el jefe de la GU no estuviera de baja, éste informara sobre determinados aspectos. Y, para el caso de que todavía estuviera de baja, y en relación a las 12.500 consultas en el SIP, efectuadas por los agentes expedientados, se requirió el testimonio del concejal o el alcalde sobre si podían acceder a dicha documentación (las 12.500 consultas al SIP); si se había realizado un análisis de riesgos para determinar las medidas para garantizar la seguridad de estos datos en los sistemas del Ayuntamiento; así como si la información vinculada a las consultas que no se consideraran ilícitas (es decir, las que no fueran objeto de los expedientes disciplinarios), había sido suprimida o bloqueada.

8. 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 el inspector jefe de la GU todavía estaba de baja.
- Que el alcalde como el concejal en el momento del informe emitido el 01/02/2019, ya no forman parte del Consistorio.
- 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 bloqueado de ningún registro ni municipal, ni supramunicipales en relación a consultas efectuadas.

9. En fecha 26/07/2021, la persona denunciante presentó un nuevo escrito en el que indicaba que el Ayuntamiento de (...) habría facilitado una lista de personas afectadas por los accesos indebidos en el SIP (efectuados por la persona aquí denunciante y otro agente) a SR. (...) (persona respecto a la cual se consultaron sus datos en el SIP).

La persona denunciante aportaba documentación diversa.

De acuerdo con los antecedentes que se han relacionado hasta aquí y con el resultado de las actuaciones de indagación llevadas a cabo en el marco de la información previa, se acuerda iniciar este procedimiento sancionador. En los siguientes apartados, se indica toda la información que exige el artículo 64.2 de la LPAC.

10. En fecha 18/10/2021, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra el Ayuntamiento de (...) por una infracción prevista en el artículo 83.4.a) en relación con los artículos 5.1.f), 32.1 y 2, todos ellos 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 (en adelante, RGPD). Este acuerdo de iniciación se notificó a la entidad imputada en fecha 20/10/2021.

11. En el acuerdo de iniciación se concedía a la entidad imputada un plazo de 10 días hábiles para formular alegaciones y proponer la práctica de pruebas que considerase convenientes para defender sus intereses. El plazo se ha superado con creces y no se han presentado alegaciones.

12. El acuerdo de iniciación explicitaba los motivos por los que no se efectuó imputación alguna respecto de otros hechos denunciados.

12.1. Sobre la entrega de informes (antecedentes 1.1 y 1.5), la resolución la directora de la Autoridad de 21/01/2021, en el procedimiento núm. PS 47/2020, sancionó al Ayuntamiento de (...) por unos hechos que junto con este hecho constituían una pluralidad de acciones en ejecución de un plan preconcebido o aprovechando una ocasión idéntica. Estas acciones infringen un mismo precepto (el art. 83.5.a del RPGD, que tipifica como infracción la vulneración del principio de licitud contemplado en los artículos 5.1.ay 6 del RGPD). Se trata de una infracción continua que ya fue sancionada por esta Autoridad. Por tanto, es de aplicación aquí el principio "non bis in idem" que se encuentra recogido en el artículo 31.1 de la LRJSP.

12. 2. Sobre la situación de baja del jefe de la GU (antecedente 1.2). Tanto los informes emitidos por el jefe de la GU como el acceso a la instancia referida son tratamientos que se habrían efectuado en ejercicio de las funciones de supervisar las operaciones del cuerpo y las actividades administrativas, que el artículo 27.1 de la Ley 16/ 1991 atribuye al frente de la GU. Lo anterior, junto con la gravedad de los hechos (que el jefe de la GU consideraba que podían ser constitutivos de ilícito penal) justificarían que, a pesar de estar de baja, el jefe de la GU emitiera dichos informes por unos hechos vinculados al SIP.

12.3. Sobre la comunicación de la incoación de los expedientes disciplinarios a las personas afectadas por los accesos al SIP ya la CUP (antecedentes 1.4, 3.2 y 9). La resolución de la directora de la APDCAT de 21/01/2021, que puso fin al procedimiento sancionador núm. PS 47/2020, sancionó al Ayuntamiento de (...) por estos mismos hechos, por lo que también resulta de aplicación aquí el principio "non bis in idem". Y en cuanto a una eventual lista de personas afectadas por los accesos ilícitos al SIP, no consta ningún elemento mínimamente indiciario que permita inferir que el Ayuntamiento hubiese difundido la citada lista. Este hecho denunciado se fundamenta en una mera suposición.

12.4. Sobre la comunicación de la incoación de los expedientes disciplinarios a los representantes sindicales (antecedente 1.3). La comunicación a la Junta de Personal del acuerdo de iniciación del expediente disciplinario incoado a la persona aquí denunciante, en los

términos que se efectuó, estaba habilitada por una norma con rango de ley (DL 1/1997), que efectúa una remisión reglamentaria. Por tanto, este tratamiento es lícito de conformidad con el artículo 6.1.c) del RGPD.

12.5. Sobre la petición de la auditoría de accesos al SIP (antecedente 1.6 y 6.1). Según informó la DGP en el marco de la información previa nº. IP 334/2020, no corresponde al interlocutor informático (que sería la persona aquí denunciante en el momento en que se pidió la auditoría) solicitar auditorías sobre los accesos al SIP, sino que las peticiones de auditorías las han solicitado de efectuar los Jefes de Policía Local. Además, 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 DGP también se sustentaría en las mismas bases jurídicas.

12.6. Sobre la encriptación del correo a través del cual se solicitó la auditoría de accesos al SIP (antecedente 6.2). La persona denunciante no aportaba copia de dicho correo, por lo que no ha sido posible comprobar si efectivamente se envió y cuál era su contenido (si incluía claves, nombres y apellidos, etc.). Tampoco se aportaba ningún mínimo indicio que permitiera inferir que, en caso de que el correo hubiera incluido los datos controvertidos, no se hubiera implementado esta medida de seguridad, que viene determinada en el Manual de Seguridad del convenio de conexión de las policías locales al SIP. Pero, incluso, en el caso no probado de que se hubiera producido la eventual infracción vinculada al envío de dicho correo electrónico sin encriptar, esta infracción ya estaba prescrita cuando se denunciaron estos hechos en fecha 15/01/ 2021. La prescripción de la infracción provoca la extinción de la responsabilidad que pudiera derivarse de la eventual conducta infractora.

Hechos probados

El Ayuntamiento de (...) no acreditó haber efectuado un análisis de 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 vinculados a las 12.500 consultas al SIP efectuadas por la persona denunciante y otro agente (todas las consultas efectuadas por éstos entre el 01/08/2017 y el mes de diciembre de 2018) que fueron objeto de auditoría (a los efectos que el Ayuntamiento investigara si fueron efectuadas por dichos agentes en el ejercicio de sus funciones o no) ya las que se refiere el informe emitido por el jefe de la GU en fecha 01/02/2019.

Fundamentos de derecho

1. Son de aplicación a este procedimiento lo que prevén la LPAC, y el artículo 15 del Decreto 278/1993, según lo que prevé la DT 2ª de la Ley 32/2010, de 1 de octubre, de la Autoridad

Catalana de Protección de Datos. De conformidad con los artículos 5 y 8 de la Ley 32/2010, la resolución del procedimiento sancionador corresponde a la directora de la Autoridad Catalana de Protección de Datos.

2. De acuerdo con el artículo 64.2.f) de la LPAC y de conformidad con lo que se indica en el acuerdo de iniciación de este procedimiento, procede dictar esta resolución sin una propuesta de resolución previa, dado que la entidad imputada no ha formulado alegaciones en el acuerdo de iniciación. Este acuerdo contenía un pronunciamiento preciso sobre la responsabilidad imputada.

2. En relación con los hechos descritos en el apartado de hechos probados, relativos a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de éstas (en adelante, RGPD), el artículo 5.1. f) del RGPD que regula el principio de integridad y confidencialidad determina que los datos personales serán "tratados de tal modo que se garantice una seguridad adecuada de las datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas".

Por su parte, el artículo 32.1 del RGPD, que prevé que "Teniendo en cuenta el estado de la técnica, las costas de aplicación, y la naturaleza, el alcance, el contexto y las fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (...)."

A su vez, el artículo 32.2 del RGPD dispone que "Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichas datos." Esto implica tener que realizar una evaluación de los riesgos que comporta cada tratamiento, para determinar las medidas de seguridad a implementar.

Durante la tramitación de este procedimiento se ha acreditado debidamente el hecho descrito en el apartado de hechos probados, que es constitutivo de la infracción prevista en el artículo 83.4.a) el RGPD, que tipifica como tal la vulneración de "las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43", entre las que se encuentra la prevista en el artículo 32 RGPD.

La conducta que aquí se aborda se ha recogido como infracción grave en el artículo 73.f) de la LOPDDDD, en la siguiente forma:

"f) La falta de adopción de las medidas técnicas y organizativas que sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos que exige el artículo 32.1 del Reglamento (UE) 2016/679."

3. El artículo 77.2 LOPDGDD dispone que, en el caso de infracciones cometidas por los responsables o encargados enumerados en el art. 77.1 LOPDGDD, la autoridad de protección de datos competente:

“(…) debe dictar una resolución que las sancione con una amonestación. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se haya cometido.

La resolución se notificará al responsable o encargado del tratamiento, a cuyo órgano dependa jerárquicamente, en su caso, ya los afectados que tengan la condición de interesado, en su caso.”

En términos similares a la LOPDDDD, el artículo 21.2 de la Ley 32/2010, determina lo siguiente:

“2. En el caso de infracciones cometidas con relación a ficheros de titularidad pública, el director o directora de la Autoritat Catalana de Protecció de Dades debe dictar una resolución que declare la infracción y establezca las medidas a adoptar para corregir sus efectos. Además, puede proponer, en su caso, la iniciación de actuaciones disciplinarias de acuerdo con lo que establece la legislación vigente sobre el régimen disciplinario del personal al servicio de las administraciones públicas. Esta resolución debe notificarse a la persona responsable del fichero o del tratamiento, a la encargada del tratamiento, si procede, al órgano del que dependan ya las personas afectadas, si las hubiere”.

En virtud de esta facultad, procede requerir al Ayuntamiento de (...) para que lo antes posible, y en todo caso en el plazo máximo de 20 días a contar desde el día siguiente de la notificación de esta resolución, realice un análisis de riesgos para determinar las medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos personales que se traten en el marco de los procedimientos disciplinarios.

Una vez adoptada la medida correctora descrita en el plazo señalado, en el plazo de los 10 días siguientes el Ayuntamiento informará de ello a la Autoridad, sin perjuicio de la facultad de inspección de esta Autoridad para efectuar las verificaciones correspondientes.

Por todo esto, resuelvo:

1. Amonestar al Ayuntamiento de (...) como responsable de una infracción prevista en el artículo 83.4.a) en relación con los artículos 5.1.f) y 32, todos ellos del RGPD.

2. Requerir al Ayuntamiento de (...) para que adopte la medida correctora señalada en el fundamento de derecho 3º y acredite ante esta Autoridad las actuaciones llevadas a cabo por cumplirla.
3. Notificar esta resolución al Ayuntamiento de (...).
4. Comunicar la resolución al Síndic de Greuges, de conformidad con lo que prevé el artículo 77.5 del LOPDDDD.
5. Ordenar que se publique esta 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 los artículos 26.2 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y 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, la entidad imputada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos Datos, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevén el artículo 123 y siguientes de la LPAC. También 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.

Si la entidad imputada manifiesta a la Autoridad su intención de interponer recurso contencioso administrativo contra la resolución firme en vía administrativa, la resolución se suspenderá cautelarmente en los términos previstos en el artículo 90.3 de la LPAC.

Igualmente, la entidad imputada podrá interponer cualquier otro recurso que estime conveniente para defender sus intereses.

La directora,