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

Identificación del expediente

Resolución de procedimiento sancionador núm. PS 56/2022, referente al Ayuntamiento de (...)

Antecedentes

1. E n fecha 31/05/2022, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de una persona por el que formulaba 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 que, en el ejercicio de sus funciones como cabo de la Policía Local de (...), en fecha 15/11/2020, mantuvo una conversación telefónica con una trabajadora del Servicio de 'Emergencias Médicas (en adelante, SEM), y denuncia el hecho de que, otro cabo de la Policía Local - con TIP (...)- accedió al registro de las grabaciones de las comunicaciones telefónicas de la Policía Local, descargó la conversación de referencia en su teléfono personal, y difundió su contenido a otros agentes y cabos del cuerpo.

A efectos de acreditar los hechos, la denuncia se acompañaba, entre otra documentación, del Acta de la Comisión para la Prevención del Acoso (en adelante, CPA) del Servicio de Recursos Humanos del Ayuntamiento de (...), de fecha 23/03/2021, en la que, a raíz de una queja interpuesta por el ahora denunciante, el cabo con TIP (...) reconocía haber accedido al contenido de la conversación mantenida entre el ahora denunciante y una trabajadora del SEM, desmentía tener una copia de la conversación, y añadía que " *en aquella época (noviembre 2020) todo el mundo tenía acceso a las grabaciones de las llamadas, ya que el anterior jefe del Departamento (ahora jubilado) había dado las llaves a casi todo el mundo de la jefatura. (...)".*
La denuncia también se acompañaba de las Actas de la CPA en las que se recogían los testigos de los agentes con TIP (...)y (...)del Ayuntamiento, en relación a los hechos que ahora se denuncian. De estos testigos, y en relación con los hechos denunciados, destaca la siguiente afirmación recogida en el acta firmada por el agente (...)" *que el sr.* [agente con TIP (...)] *comentó públicamente en una conversación que había escuchado una grabación de una intervención policial del día 15 de noviembre donde el señor [* ahora denunciante] *proponía a la persona con la que hablaba de que tramitara una queja contra los compañeros de la policía (...)".*

2. La Autoridad abrió una fase de información previa (núm. IP 206/2022), 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 13/06/2022 se requirió a la entidad denunciada para que, entre otros, aportara el registro de acceso a las grabaciones telefónicas efectuadas por la Policía Local en el período comprendido entre el mes de noviembre a diciembre de 2020, indicara las personas concretas que disponían de credenciales que permitían el acceso a las grabaciones telefónicas registradas por la Policía Local, argumentando los motivos por los que el agente con TIP (...) reveló a determinados agentes el contenido de la conversación telefónica mantenida con el ahora denunciante y una trabajadora del SEM.

4. En fecha 28/06/2022, el Ayuntamiento respondió el requerimiento mencionado a través de escrito en el que exponía lo siguiente:

- " *El Ayuntamiento no dispone de la relación de las personas concretas, que prestaban servicio a la Policía Local en el período noviembre-diciembre de 2020, que disponían de credenciales (usuario y contraseña personal) que les permitía el acceso a las grabaciones telefónicas registradas por la Policía Local. Sin embargo, durante el período noviembre-diciembre de 2020 únicamente determinados cabos de la Policía Local, entre los que figuraba el señor* [agente con TIP (...)] *, disponían de código de acceso, proporcionado por el anterior jefe de la Policía Local, que actualmente no presta servicios al Ayuntamiento de (...), para el ejercicio atribuciones profesionales encomendadas.*
- *Os confirmamos que el inspector jefe de la Policía Local era una de las personas que disponía de las credenciales para acceder a las grabaciones telefónicas (…).*
- *El Ayuntamiento no dispone del registro de acceso a las grabaciones efectuadas por la Policía Local, en el período comprendido entre los meses de noviembre-diciembre de 2020, dado el tiempo transcurrido ya que las llamadas y registro únicamente se almacenan por un período máximo de un mes. Pasado este plazo, los datos se eliminan. (...)*
- *La conservación telefónica con una trabajadora del Servicio de Emergencias Médicas, en relación con un accidente de tráfico, no fue descargada por parte del cabo, señor [* agente con TIP (...)] *, sino que únicamente fue escuchada en el marco de las funciones profesionales atribuidas de seguimiento del servicio prestado por la Policía Local de (...) en el citado accidente de tráfico.*

En último término, la entidad reclamada exponía que desde la Policía Local se tenía constancia de que los miembros del SEM pidieron telefónicamente explicaciones de "la *actuación policial de auxilio inadecuada en dicho accidente* " y añadían que " *fue necesaria la revisión de la conversación y en la que se pudo constatar que el interlocutor de la Policía Local que atendió la llamada, el cabo [* ahora denunciante], *actuó de forma incorrecta y no como se espera de un cabo de la Policía Local. Verbalizó valoraciones negativas del servicio de la Policía Local e hizo manifestaciones de un servicio efectuado por la Policía Local en un accidente de tráfico en el que no había participado. Asimismo, incitaba a que el Servicio de Emergencias Médicas interpusiera la denuncia o queja correspondiente a raíz de la actuación de los agentes de la Policía Local intervinientes, entre ellos el cabo [* con TIP (...)], *en el servicio de auxilio del accidente. (...)".*

En último término, el Ayuntamiento ponía de manifiesto que los motivos por los que se llevó a cabo el acceso a la referida conversación telefónica, no fue otro que conocer los motivos por los que el SEM había pedido explicaciones a la Policía Local , en relación con un determinado incidente.

5. En fecha 22/07/2022, también en el seno de esta fase de información previa, el Área de Inspección de la Autoridad requirió a la entidad denunciada para que aportara la copia del análisis de riesgos vigente entre los meses de noviembre de 2020 y enero de 2021. Asimismo, se requería al Ayuntamiento para que informara sobre qué apartado del documento concreto, analiza el detalle de las actividades que debían ser objeto de registro, de acuerdo con el Esquema Nacional de Seguridad (en adelante, ENS).

6. En fecha 02/08/2022, y aún en el marco de la fase de información previa, el Ayuntamiento de (...) dio respuesta a dicho requerimiento, afirmando no disponer de un análisis de riesgos vigente entre los meses de noviembre de 2020 y enero de 2021.

7. En fecha 22/09/2022, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra el Ayuntamiento de (...) por tres presuntas infracciones: dos infracciones previstas en el artículo 83.4 .a) en relación con los apartados 1º y 2º del artículo 32, respectivamente; y, una tercera infracción prevista en el artículo 83.5.a) en relación con el artículo 5.1 f); 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 23/09/2022.

8. El acuerdo de iniciación explicitaba los motivos por los que no se efectuó imputación alguna respecto al hecho denunciado, relativo a la presunta descarga por parte del agente con TIP (...) de la conversación mantenida por el aquí denunciando con una trabajadora del SEM, en su móvil particular. En síntesis, se procedió al archivo de este hecho dado que, aparte de las manifestaciones del ahora denunciante, no se disponía de otro elemento que pudiera corroborar que el agente descargó la referida conversación y la guardar en su dispositivo móvil, descarga que, por otra parte, el Ayuntamiento negó que se hubiera producido. Al respecto, al no poder acreditar este hecho denunciado, resulta de aplicación el principio de presunción de inocencia.

9. 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.

10. En fecha 10/10/2022, el Ayuntamiento de (...) formuló alegaciones al acuerdo de iniciación , que se abordan en el apartado 2 de los fundamentos de derecho.

11. En fecha 15/12/2022, la persona instructora de este procedimiento formuló una propuesta de resolución, por la que proponía que la directora de la Autoridad Catalana de Protección de Datos amonestara al Ayuntamiento de (...) como responsable, de dos infracciones previstas en el artículo 83.4.a) en relación con los apartados 1º y 2º del artículo 32.1, respectivamente; y una tercera infracción prevista en el artículo 83.5.a) en relación con el artículo 5.1 f), todos ellos del RGPD.

Esta propuesta de resolución se notificó en fecha 16/12/2022 y se concedía un plazo de 10 días para formular alegaciones.

12. El plazo se ha superado con creces y no se han presentado alegaciones.

Hechos probados

1. El Ayuntamiento de (...) no adoptó las medidas de seguridad y técnicas requeridas de acuerdo con el ENS, lo que propició que, durante un período indeterminado, que al menos comprende los meses de noviembre y diciembre de 2020, el Ayuntamiento desconociera qué personas disponían de las credenciales que permitían el acceso a las grabaciones telefónicas registradas por la Policía Local, y no conservara el registro de las personas que accedían a las referidas conversaciones telefónicas transcurrido un mes desde la realización de la llamada.

2. El Ayuntamiento de (...) durante los meses de noviembre 2020 a enero de 2021 no disponía del correspondiente análisis de riesgos, en relación a los datos personales que trataba.

3. El cabo de la Policía Local con TIP (...)del Ayuntamiento de (...) difundió públicamente el contenido de la conversación telefónica mantenida por el ahora denunciante con una trabajadora del SEM, sin que el Ayuntamiento haya acreditado o justificado que las personas que tuvieron conocimiento de la referida información, a raíz de su difusión por parte del cabo, estuvieran autorizadas para acceder al contenido de las grabaciones telefónicas registradas. Esta difusión se llevó a cabo en fecha indeterminada, pero posterior al día 15/11/2020, fecha en que tuvo lugar la referida conversación telefónica.

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 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. La entidad imputada no ha formulado alegaciones a la propuesta de resolución, pero sí lo hizo en el acuerdo de iniciación. Al respecto, se considera oportuno reiterar a continuación lo más relevante de la respuesta motivada de la persona instructora a estas alegaciones.

2.1 Sobre el hecho probado primero.

El escrito de alegaciones presentado en fecha 10/10/2022, en el acuerdo de iniciación del presente procedimiento, ponía de manifiesto las siguientes consideraciones:

- Que, respecto al acceso al contenido de las grabaciones telefónicas registradas por la Policía Local, " *el sistema dispone de doble factor de autenticación y se requiere de fichero clave de acceso para acceder*" .

-Que " *el anterior inspector facilitó los permisos de acceso a las grabaciones telefónicas registradas por la Policía Local únicamente a los cabos y, a raíz de las funciones de seguimiento del servicio prestado por la Policía Local de (...) en el accidente de tráfico, el cabo (...) [TIP (...)] escuchó la grabación. Esto fue motivado porque miembros del Servicio de Emergencias Médicas habían pedido explicaciones de la actuación policial de auxilio inadecuada en el accidente de tráfico".*

- Que *"a raíz de esta actuación en el accidente de tráfico y para evitar cualquier tipo de incidente con las grabaciones telefónicas, de forma preventiva, el inspector de la Policía Local decidió cambiar el sistema de permisos de acceso a las grabaciones de los cabos. Desde entonces y hasta la actualidad, la única persona autorizada para acceder a las grabaciones telefónicas es el Inspector de la Policía Local del Ayuntamiento de (...), que tiene acceso por medio de usuario y contraseña. Asimismo, el fichero clave que permite poner en marcha el servicio sólo está instalado en el ordenador de sobremesa situado en el despacho del Inspector de la Policía Local. Este ordenador de sobremesa está instalado en dominio Windows Server protegido, a su vez, por usuario y contraseña. Además, el acceso al despacho del Inspector de la Policía está protegido con llave".*

Pues bien, en primer término, cabe señalar que, tal y como manifestaba la persona instructora en la propuesta de resolución, la entidad imputada no cuestiona el primero de los hechos imputados en este procedimiento, referido a la falta de medidas de seguridad y técnicas requeridas de de acuerdo con el ENS. De hecho, la Corporación admite que, a raíz del incidente de referencia, se decidió cambiar el sistema de permisos de acceso a las grabaciones telefónicas, por lo que la única persona autorizada para acceder es el Inspector de la Policía Local. En relación con lo anterior, el Ayuntamiento también ha puesto de manifiesto que, el fichero que permite el acceso a las grabaciones de las conversaciones telefónicas, sólo se encuentra instalado en el ordenador del Inspector de la Policía Local, en dominio Windows Server, protegido por usuario y contraseña, y que este ordenador se encuentra ubicado en el despacho del Inspector, cuyo acceso está protegido con clave.

De acuerdo con el ENS, toda organización debe poder establecer de forma clara la trazabilidad de los accesos a datos personales, en este caso, a las grabaciones de conversaciones telefónicas (quién, cuándo, a qué información, etcétera), cosa que no ocurría en el caso analizado en el que, tal y como se ha expuesto en el apartado de hechos probados, y se argumentó en la propuesta de resolución, no se disponía de un registro que recogiera esta información. Por otra parte, el Ayuntamiento tampoco garantizó que las credenciales de acceso al sistema estuvieran siempre bajo control exclusivo de sus usuarios, lo que impedía que se pudiera tener información cierta sobre la persona o personas que accedían a los datos.

2.2 . Sobre el hecho probado segundo .

Dado que el Ayuntamiento ha reconocido los hechos imputados, mediante escrito presentado ante la Autoridad en fecha 02/08/2022 – antecedente 6º– resulta innecesario realizar ninguna consideración adicional al respecto, sin perjuicio de lo que se dirá en el Fundamento de derecho 3º, sobre la calificación jurídica que merecen dichos hechos.

2.3 Sobre el hecho probado tercero.

Respecto a la actuación del cabo de la Policía Local con TIP (...)que difundió públicamente el contenido de la conversación mantenida por el aquí denunciante con una trabajadora del SEM, la entidad imputada argumentaba lo siguiente:

- Que *"el Cabo de la Policía Local con TIP (...), (...), del Ayuntamiento de (...) accedió a la grabación de la llamada pero no se dispone de evidencias de que permitan afirmar que difundiera públicamente el contenido de la conversación (...)"*

- Que " *la actuación del cabo (...)* [el aquí denunciante] *(...), en relación a la conversación con el Servicio de Emergencia Médicas a raíz del accidente de tráfico, fue conocida por los integrantes del cuerpo de la Policía Local. Sin embargo, esto no implica que los agentes accedieran a la grabación de la llamada y no se descarta que tuvieran conocimiento por su propio cabo (...)* [el aquí denunciante].

En resumen, el Ayuntamiento de (...) defendía que no existen evidencias que permitan sostener que el Caporal de la Policía Local con TIP (...) difundió a otros agentes el contenido de la conversación telefónica, y añad ya que, no se puede descartar que tuvieran acceso por el propio Caporal [aquí denunciante].

En relación con lo anterior, es oportuno señalar que, tal y como se transcribe en el antecedente primero de esta resolución, las actas de la CPA del Servicio de Recursos Humanos del Ayuntamiento de (...), de fecha 23/03/2021, recogen los testigos de los agentes con TIP (...)y (...)del Ayuntamiento, y en una de ellas -concretamente la firmada por el agente TIP (...)- se hace constar de forma literal que *"D. [agente con TIP (...)] comentó públicamente en una conversación que había escuchado una grabación de una intervención policial del día 15 de noviembre donde el señor [ahora denunciante] proponía a la persona con la que hablaba de que tramitara una queja contra los compañeros de la policía (...)"* . Al respecto, también se hace pertinente remarcar que, en la fase de información previa, el Ayuntamiento no cuestionó este hecho.

En definitiva, ante la alegación de la entidad denunciada negando la existencia de evidencias que permitan sostener la difusión de la información controvertida por parte del agente con TIP (...) a otros agentes, ésta Autoridad no puede desconocer que, aparte de las afirmaciones del aquí denunciante, existe un acta de la CPA, firmada por un agente de la Policía Local, que confirma tal difusión; testigo que, cabe remarcar, la entidad imputada no ha desvirtuado, ni en la fase de información previa que precedió a este procedimiento sancionador, ni tampoco en el seno de éste.

Por lo expuesto, las alegaciones formuladas por el Ayuntamiento no pueden tener éxito.

3. En relación con los hechos descritos en el punto 1º del apartado de hechos probados, se debe acudir al artículo 5.1 f) del RGPD, que regula el principio de integridad y de confidencialidad, y determina que los datos personales deben ser " *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, en lo referente a la seguridad de los datos, dispone lo siguiente:

> *"1. 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, que en su caso incluya, entre otros:*
> *a. La seudonimización y el cifrado de datos personales;*

b. *La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
c. *La capacidad de restaurar la disponibilidad y el acceso a las datos personales de forma rápida en caso de incidente físico o técnico;*
d. *Un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

A este respecto, la disposición adicional primera de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD) establece lo siguiente:

"1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, con la adaptación de los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/769.
2. Los responsables que enumera el artículo 77.1 de esta Ley orgánica aplicarán a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones sujetas al derecho privado vinculadas a aquellos (...)."

Los preceptos transcritos establecen la obligación del responsable del tratamiento, en este caso el Ayuntamiento de (...), de adoptar las medidas de seguridad apropiadas a fin de garantizar un nivel de seguridad adecuado al riesgo.

En el caso que aquí nos ocupa, es necesario tener en cuenta las medidas de seguridad que preveía el ENS, aprobado por el Real Decreto 3/2010, de 8 de enero, vigente en el momento de la comisión de los hechos. En concreto, los artículos 13, 14.1, 16 y 23 del referido ENS, preveían lo siguiente (el subrayado es nuestro):

Artículo 13. Análisis y gestión de los riesgos
1. *Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.*
2. *Esta gestión se realizará mediante la análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.*
3. *Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en cualquier caso, existirá una proporcionalidad entre ellas y los riesgos.*

Articulo 14. Gestión de personal
(…)
4. *Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.*

Artículo 16. Autorización y control de los accesos
El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

Artículo 23. Registro de actividad.
Con la finalidad exclusiva de conseguir el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar ya la propia imagen de los afectados, y de acuerdo con la normativa sobre protección y datos personales , de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Asimismo, cabe señalar que la Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña, a su disposición adicional undécima, sobre la gestión de la documentación y archivo de los documentos electrónicos, establece lo siguiente:

"5. Los sistemas de información que utilicen las administraciones públicas incluidas en el ámbito de aplicación de la presente ley deben garantizar, siempre que sea posible, la autenticidad y la integridad de sus datos, así como la trazabilidad de las acciones que lleven a cabo".

Durante la tramitación de este procedimiento se ha acreditado debidamente el hecho descrito en el punto primero del apartado de los hechos probados, consistente en la falta de adopción de las medidas técnicas y de seguridad necesarias , que se considera constitutivo de la infracción prevista en el artículo 83.4.a) el RGPD, que tipifica la vulneración de *" las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 42"* , entre las que se encuentra la prevista en el artículo 32.1 del 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:

"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 del Reglamento (UE) 2016/679."

4. Con respecto al hecho descrito en el punto 2º del apartado de hechos probados, en lo referente a la falta de realización de un análisis de riesgos, también es necesario acudir al artículo 5.1.f) del RGPD, transcrito al primer punto de la calificación jurídica de los hechos.

A su vez, el apartado segundo del artículo 32 del RGPD, en relación con el análisis de riesgos, establece lo siguiente:

"2. 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 autorizado a dichas datos".

También el artículo 28 de la LOPDDDD prevé la obligación del responsable del tratamiento de adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar y acreditar

que el tratamiento es conforme al RGPD, teniendo en cuenta, en particular, los riesgos que se transcriben a continuación:

> *"2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los riesgos superiores que pueden producirse en los siguientes supuestos: a) Cuando el tratamiento pueda generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la pseudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados .*
> *b) Cuando el tratamiento pueda privar a los afectados de sus derechos y libertades o pueda impedirles el ejercicio del control sobre sus datos personales.*
> *c) Cuando se produzca el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta Ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.*
> *d) Cuando el tratamiento implique una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de éstos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.*
> *e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en una situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.*
> *f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o comporte la recogida de una gran cantidad de datos personales.*
> *g) Cuando los datos personales deban ser objeto de transferencia, con carácter habitual, a terceros estados u organizaciones internacionales respecto de los cuales no se haya declarado un nivel adecuado de protección.*
> *h) Cualesquiera otras que a juicio del responsable o del encargado puedan tener relevancia y en particular los previstos en códigos de conducta y estándares definidos por esquemas de certificación."*

artículo 83.4 del 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 32.2 RGPD.

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

> *"p) El tratamiento de datos personales sin llevar a cabo una valoración previa de los elementos mencionados en el artículo 28 de esta Ley orgánica."*

5. En cuanto a la conducta descrita en el punto 3º de los hechos imputados, en lo referente a la divulgación del contenido de una conversación telefónica, también es necesario acudir al artículo 5.1 f) del RGPD, transcrito al primer punto de la calificación jurídica de los hechos.

Por su parte, el artículo 5 de la LOPDDDD, relativo al deber de confidencialidad, dispone:

"1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase del mismo están sujetos al deber de confidencialidad a que se refiere el artículo 5.1. f) del Reglamento (UE) 2016/679.
2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.
3. Las obligaciones establecidas en los apartados anteriores se mantienen aunque haya finalizado la relación del obligado con el responsable o encargado del tratamiento".

Este hecho imputado es constitutivo de infracción, según lo previsto en el artículo 83.5 a) del RGPD, que tipifica como tal, la vulneración de los " *a) Los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5,6, 7 y 9* ", entre los que se encuentra el principio de confidencialidad.

A su vez, esta conducta se ha recogido como infracción muy grave en el artículo 72.1 i) del LOPDDDD en la siguiente forma:

"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquél y, en particular las siguientes: i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica".

6. 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 Autoridad Catalana de Protección de Datos debe dictar una resolución que declare la infracción y establezca las medidas a adoptar para corregir sus efectos . (...)".

En virtud de esta facultad, procede requerir al Ayuntamiento de (...) para que lo antes posible, y en todo caso en el plazo máximo de 10 días a contar desde el día siguiente de la notificación de esta resolución, implemente las medidas correctoras que se indican a continuación:

6.1 Respecto a los hechos descritos en el 1er punto del apartado de hechos probados, acredite disponer de un registro de accesos al sistema que almacena las grabaciones de las conversaciones telefónicas mantenidas por la Policía Local.

6.2 Respecto a los hechos descritos en el 2º punto del apartado de hechos probados, documente el análisis de riesgos referidos a los tratamientos vinculados a la grabación de las llamadas telefónicas de la Policía Local y de las conversaciones mantenidas a través de los equipos de transmisiones de el Ayuntamiento.

Una vez adoptadas las medidas correctoras descritas, en los plazos señalados, es necesario que en los 10 días siguientes el Ayuntamiento de (...) informe a la Autoridad, sin perjuicio de la facultad de inspección de la misma Autoridad para realizar las verificaciones correspondientes.

Respecto a los hechos descritos en el 3r punto del apartado de hechos probados, procede descartar la adopción de medidas correctoras dado que se trata de un hecho puntual y consumado.

Por todo esto, resuelvo:

1. Amonestar al Ayuntamiento de (...) como responsable de tres infracciones: dos infracciones previstas en el artículo 83.4.a) en relación con los apartados 1º y 2º del artículo 32, respectivamente; y, una tercera infracción prevista en el artículo 83.5.a) en relación con el artículo 5.1.f), todos ellos del RGPD.

2. Requerir al Ayuntamiento de (...) para que adopte las medidas correctoras señaladas en el fundamento de derecho 6º y acredite ante esta Autoridad las actuaciones llevadas a cabo para cumplirlas.

3. Notificar esta resolución a la Alcaldía 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,