

En aquesta resolució s'han ocultat les mencions a l'entitat afectada per tal de donar compliment a l'art. 17.2 de la Llei 32/2010, atès que en cas de revelar el nom de l'entitat afectada, es podrien identificar també les persones físiques afectades.

Identificació de l'expedient

Resolució del procediment sancionador núm. PS 56/2022, referent a l'Ajuntament de (...)

Antecedents

1. En data 31/05/2022, va tenir entrada a l'Autoritat Catalana de Protecció de Dades un escrit d'una persona pel qual formulava denúncia contra l'Ajuntament de (...), amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals.

En concret, la persona denunciant exposava que, en l'exercici de les seves funcions com a caporal de la Policia Local de (...), en data 15/11/2020, va mantenir una conversació telefònica amb una treballadora del Servei d'Emergències Mèdiques (en endavant, SEM), i denuncia el fet que, un altre caporal de la Policia Local – amb TIP (...) - va accedir al registre de les gravacions de les comunicacions telefòniques de la Policia Local, va descarregar la conversa de referència en el seu telèfon personal, i va difondre'n el contingut a altres agents i caporals del cos.

Als efectes d'acreditar els fets, la denúncia s'acompanyava, entre d'altra documentació, de l'Acta de la Comissió per a la Prevenció de l'Assetjament (en endavant, CPA) del Servei de Recursos Humans de l'Ajuntament de (...), de data 23/03/2021, en la qual, arran d'una queixa interposada per l'ara denunciant, el caporal amb TIP (...) reconeixia haver accedit al contingut de la conversa mantinguda entre l'ara denunciant i una treballadora del SEM, desmentia tenir una còpia de la conversa, i afegia que *“en aquella època (novembre 2020) tothom tenia accés a les gravacions de les trucades, ja que l'anterior cap del Departament (ara jubilat) havia donat les claus a gairebé tothom de la prefectura. (...)”*.

La denúncia també s'acompanyava de les Actes de la CPA en les que es recullen els testimonis dels agents amb TIP (...) i (...) de l'Ajuntament, en relació amb els fets que ara es denuncien. D'aquests testimonis, i en relació amb els fets denunciats, destaca la següent afirmació recollida en l'acta signada per l'agent (...) *“que el Sr. [agent amb TIP (...)] va comentar públicament en una conversa que havia escoltat una gravació d'una intervenció policial del dia 15 de novembre on el senyor [ara denunciant] proposava a la persona amb que parlava que tramités una queixa contra els companys de la policia (...)”*.

2. L'Autoritat va obrir una fase d'informació prèvia (núm. IP 206/2022), d'acord amb el que preveu l'article 7 del Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat, i l'article 55.2 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (d'ara endavant, LPAC), per determinar si els fets eren susceptibles de motivar la incoació d'un procediment sancionador.

3. En aquesta fase d'informació, en data 13/06/2022 es va requerir l'entitat denunciada perquè, entre d'altres, aportés el registre d'accés a les gravacions telefòniques efectuades per la Policia Local en el període comprès entre el mes de novembre a desembre de 2020, indiqués les persones concretes que disposaven de credencials que permetien l'accés a les

gravacions telefòniques enregistrades per la Policia Local, i argumentés els motius pels quals l'agent amb TIP (...) va revelar a determinats agents el contingut de la conversa telefònica mantinguda amb l'ara denunciant i una treballadora del SEM.

4. En data 28/06/2022, l'Ajuntament va respondre el requeriment esmentat a través d'escrit en què exposava el següent:

- *“L'Ajuntament no disposa de la relació de les persones concretes, que prestaven servei a la Policia Local en el període novembre-desembre de 2020, que disposaven de credencials (usuari i contrasenya personal) que els hi permetia l'accés a les gravacions telefòniques enregistrades per la Policia Local. No obstant això, durant el període novembre-desembre de 2020 únicament determinats caporals de la Policia Local, entre els que figurava el senyor [agent amb TIP (...)], disposaven de codi d'accés, proporcionat per l'anterior cap de la Policia Local, el qual actualment no presta serveis a l'Ajuntament de (...), per a l'exercici atribucions professionals encomanades.*
- *Us confirmem que l'inspector en cap de la Policia Local era una de les persones que disposava de les credencials per accedir a les gravacions telefòniques (...).*
- *L'Ajuntament no disposa del registre d'accés a les gravacions efectuades per la Policia Local, en el període comprès entre els mesos de novembre-desembre de 2020, atès el temps transcorregut ja que les trucades i registre únicament s'emmagatzemen per un període màxim d'un mes. Passat aquest termini les dades s'eliminen. (...)*
- *La conservació telefònica amb una treballadora del Servei d'Emergències Mèdiques, en relació amb un accident de trànsit, no va ser descarregada per part del caporal, senyor [agent amb TIP (...)], sinó que únicament va ser escoltada en el marc de les funcions professionals atribuïdes de seguiment del servei prestat per la Policia Local de (...) en l'esmentat accident de trànsit.*

En darrer terme, l'entitat reclamada exposava que des de la Policia Local es tenia constància que els membres del SEM van demanar telefònicament explicacions de *“l'actuació policial d'auxili inadequada en l'esmentat accident”* i afegien que *“va ser necessària la revisió de la conversa i en què es va poder constatar que l'interlocutor de la Policia Local que va atendre la trucada, el caporal [ara denunciant], va actuar de manera incorrecta i no com s'espera d'un caporal de la Policia Local. Va verbalitzar valoracions negatives del servei de la Policia Local i va fer manifestacions d'un servei efectuat per la Policia Local en un accident de trànsit en què no havia participat. Així mateix, incitava a què el Servei d'Emergències Mèdiques interposés la denúncia o queixa corresponent arran de l'actuació dels agents de la Policia Local intervinents, entre ells el caporal [amb TIP (...)], en el servei d'auxili de l'accident. (...)”*.

En darrer terme, l'Ajuntament posava de manifest que els motius pels quals es va dur a terme l'accés a la referida conversa telefònica, no va ser altre que el de conèixer els motius pels quals el SEM havia demanat explicacions a la Policia Local, en relació amb un determinat incident.

5. En data 22/07/2022, també en el si d'aquesta fase d'informació prèvia, l'Àrea d'Inspecció de l'Autoritat va requerir l'entitat denunciada perquè aportés la còpia de l'anàlisi de riscos vigent entre els mesos de novembre de 2020 i gener de 2021. Així mateix, es requeria l'Ajuntament perquè informés sobre quin apartat del document concret, analitza el detall de les activitats que havien de ser objecte de registre, d'acord amb l'Esquema Nacional de Seguretat (en endavant, ENS).

6. En data 02/08/2022, i encara en el marc de la fase d'informació prèvia, l'Ajuntament de (...) va donar resposta al requeriment esmentat, afirmant no disposar d'un anàlisi de riscos vigent entre els mesos de novembre de 2020 i gener de 2021.

7. En data 22/09/2022, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra l'Ajuntament de (...) per tres presumptes infraccions: dues infraccions previstes a l'article 83.4.a) en relació amb els apartats 1r i 2n de l'article 32, respectivament; i, una tercera infracció prevista a l'article 83.5.a) en relació amb l'article 5.1 f); tots ells del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes (en endavant, RGPD). Aquest acord d'iniciació es va notificar a l'entitat imputada en data 23/09/2022.

8. L'acord d'iniciació explicitava els motius pels quals no es va efectuar cap imputació respecte al fet denunciat, relatiu a la presumpta descàrrega per part de l'agent amb TIP (...) de la conversació mantinguda per l'aquí denunciant amb una treballadora del SEM, al seu mòbil particular. En síntesi, es va procedir a l'arxiu d'aquest fet atès que, a banda de les manifestacions de l'ara denunciant, no es disposava de cap altre element que pogués corroborar que l'agent va descarregar la referida conversa i la va desar al seu dispositiu mòbil, descarrega que, d'altra banda, l'Ajuntament va negar que s'hagués produït. Al respecte, en no poder acreditar aquest fet denunciat, resulta d'aplicació el principi de presumpció d'innocència.

9. A l'acord d'iniciació es concedia a l'entitat imputada un termini de 10 dies hàbils per formular al·legacions i proposar la pràctica de proves que considerés convenientes per defensar els seus interessos.

10. En data 10/10/2022, l'Ajuntament de (...) va formular al·legacions a l'acord d'iniciació, que s'aborden a l'apartat 2 dels fonaments de dret.

11. En data 15/12/2022, la persona instructora d'aquest procediment va formular una proposta de resolució, per la qual proposava que la directora de l'Autoritat Catalana de Protecció de Dades amonestés l'Ajuntament de (...) com a responsable, de dues infraccions previstes a l'article 83.4.a) en relació amb els apartats 1r i 2n de l'article 32.1, respectivament; i una tercera infracció prevista a l'article 83.5.a) en relació amb l'article 5.1 f), tots ells de l'RGPD.

Aquesta proposta de resolució es va notificar en data 16/12/2022 i es concedia un termini de 10 dies per formular al·legacions.

12. El termini s'ha superat amb escreix i no s'han presentat al·legacions.

Fets provats

1. L'Ajuntament de (...) no va adoptar les mesures de seguretat i tècniques requerides d'acord amb l'ENS, fet que va propiciar que, durant un període indeterminat, que com a mínim comprèn els mesos de novembre i desembre de 2020, l'Ajuntament desconegués quines persones disposaven de les credencials que permetien l'accés a les gravacions

telefòniques enregistrades per la Policia Local, i no conservés el registre de les persones que accedien a les referides conversacions telefòniques transcorregut un mes des de la realització de la trucada.

2. L'Ajuntament de (...) durant els mesos de novembre 2020 a gener de 2021 no disposava del corresponent anàlisi de riscos, en relació amb les dades personals que tractava.
3. El caporal de la Policia Local amb TIP (...) de l'Ajuntament de (...) va difondre públicament el contingut de la conversa telefònica mantinguda per l'ara denunciada amb una treballadora del SEM, sense que l'Ajuntament hagi acreditat o justificat que les persones que van tenir coneixement de la referida informació, arran de la seva difusió per part del caporal, estiguessin autoritzades per accedir al contingut de les gravacions telefòniques enregistrades. Aquesta difusió es va dur a terme en una data indeterminada, però posterior al dia 15/11/2020, data en què va tenir lloc la referida conversa telefònica.

Fonaments de dret

1. Són d'aplicació a aquest procediment el que preveuen l'LPAC, i l'article 15 del Decret 278/1993, segons el que preveu la DT 2a de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades. De conformitat amb els articles 5 i 8 de la Llei 32/2010, la resolució del procediment sancionador correspon a la directora de l'Autoritat Catalana de Protecció de Dades.
2. L'entitat imputada no ha formulat al·legacions a la proposta de resolució, però sí que ho va fer a l'acord d'iniciació. Respecte d'això, es considera oportú reiterar a continuació el més rellevant de la resposta motivada de la persona instructora a aquestes al·legacions.

2.1 Sobre el fet provat primer.

L'escrit d'al·legacions presentat en data 10/10/2022, a l'acord d'iniciació del present procediment, posava de manifest les següents consideracions:

- Que, respecte l'accés al contingut de les gravacions telefòniques enregistrades per la Policia Local, *"el sistema disposa de doble factor d'autenticació i es requereix de fitxer clau d'accés per accedir-hi"*.
- Que *"l'anterior inspector va facilitar els permisos d'accés a les gravacions telefòniques enregistrades per la Policia Local únicament als caporals i, arran de les funcions de seguiment del servei prestat per la Policia Local de (...) en l'accident de trànsit, el caporal (...) [TIP (...)] va escoltar la gravació. Això va ser motivat perquè membres del Servei d'Emergències Mèdiques havien demanat explicacions de l'actuació policial d'auxili inadequada en l'accident de trànsit"*.
- Que *"arran d'aquesta actuació en l'accident de trànsit i per evitar qualsevol tipus d'incident amb les gravacions telefòniques, de manera preventiva, l'inspector de la Policia Local va decidir canviar el sistema de permisos d'accés a les gravacions dels caporals. Des d'aleshores i fins a l'actualitat, l'única persona autoritzada per accedir a les gravacions telefòniques és l'Inspector de la Policia Local de l'Ajuntament de (...), que hi té accés per mitjà d'usuari i contrasenya. Així mateix, el fitxer clau que permet posar en marxa el servei només està instal·lat a l'ordinador de sobretaula situat al despatx de l'Inspector de la Policia*

Local. Aquest ordinador de sobretaula està instal·lat en domini Windows Server protegit, a la vegada, per usuari i contrasenya. A més a més, l'accés al despatx de l'Inspector de la Policia està protegit amb clau".

Doncs bé, en primer terme, escau assenyalar que, tal com manifestava la persona instructora en la proposta de resolució, l'entitat imputada no qüestiona el primer dels fets imputats en aquest procediment, referit a la manca de mesures de seguretat i tècniques requerides d'acord amb l'ENS. De fet, la Corporació admet que, arran de l'incident de referència, es va decidir canviar el sistema de permisos d'accés a les gravacions telefòniques, de manera que l'única persona autoritzada per accedir-hi és l'Inspector de la Policia Local. En relació amb l'anterior, l'Ajuntament també ha posat de manifest que, el fitxer que permet l'accés als enregistraments de les converses telefòniques, només es troba instal·lat a l'ordinador de l'Inspector de la Policia Local, en domini Windows Server, protegit per usuari i contrasenya, i que aquest ordinador es troba ubicat al despatx de l'Inspector, l'accés al qual, està protegit amb clau.

D'acord amb l'ENS, tota organització ha poder establir de forma clara la traçabilitat dels accessos a dades personals, en aquest cas, als enregistraments de converses telefòniques (qui, quan, a quina informació, etcètera), cosa que no ocorria en el cas analitzat en què, tal com s'ha exposat a l'apartat de fets provats, i s'argumentà en la proposta de resolució, no es disposava d'un registre que recollís aquesta informació. D'altra banda, l'Ajuntament tampoc no va garantir que les credencials d'accés al sistema estiguessin sempre sota control exclusiu dels seus usuaris, fet que impedia que es pogués tenir informació certa sobre la persona o persones que accedien a les dades.

2.2 . Sobre el fet provat segon.

Atès que l'Ajuntament ha reconegut els fets imputats, per mitjà d'escrit presentat davant l'Autoritat en data 02/08/2022 – antecedent 6è– resulta innecessari fer cap consideració addicional al respecte, sens perjudici del que es dirà en el Fonament de dret 3r, sobre la qualificació jurídica que mereixen els dits fets.

2.3 Sobre el fet provat tercer.

Respecte l'actuació del caporal de la Policia Local amb TIP (...) que va difondre públicament el contingut de la conversa mantinguda per l'aquí denunciant amb una treballadora del SEM, l'entitat imputada argumentava el següent:

- Que "el Caporal de la Policia Local amb TIP (...), (...), de l'Ajuntament de (...) va accedir a l'enregistrament de la trucada però no es disposa d'evidències que permetin afirmar que difongués públicament el contingut de la conversa (...)"

- Que "l'actuació del caporal (...) [l'aquí denunciant] (...), en relació a la conversa amb el Servei d'Emergència Mèdiques arran de l'accident de trànsit, va ser coneguda pels integrants del cos de la Policia Local. No obstant, això no implica que els agents accedissin a l'enregistrament de la trucada i no es descarta que en tinguessin coneixement pel propi caporal (...) [l'aquí denunciant]."

En resum, l'Ajuntament de (...) defensava que no existeixen evidències que permetin sostenir que el Caporal de la Policia Local amb TIP (...) va difondre a d'altres agents el

contingut de la conversa telefònica, i afegia que, no es pot descartar que hi tinguessin accés pel propi Caporal [aquí denunciant].

En relació amb l'anterior, és oportú assenyalar que, tal i com es transcriu a l'antecedent primer d'aquesta resolució, les actes de la CPA del Servei de Recursos Humans de l'Ajuntament de (...), de data 23/03/2021, recullen els testimonis dels agents amb TIP (...)i (...)de l'Ajuntament, i en una d'elles -concretament la signada per l'agent TIP (...) - s'hi fa constar de forma literal que "el Sr. [agent amb TIP (...)] va comentar públicament en una conversa que havia escoltat una gravació d'una intervenció policial del dia 15 de novembre on el senyor [ara denunciant] proposava a la persona amb que parlava que tramités una queixa contra els companys de la policia (...)". Al respecte, també es fa pertinent remarcar que, en la fase d'informació prèvia, l'Ajuntament no va qüestionar aquest fet.

En definitiva, davant l'al·legació de l'entitat denunciada negant l'existència d'evidències que permetin sostenir la difusió de la informació controvertida per part de l'agent amb TIP (...)a d'altres agents, aquesta Autoritat no pot desconèixer que, a banda de les afirmacions de l'aquí denunciant, existeix una acta de la CPA, signada per un agent de la Policia Local, que confirma tal difusió; testimoni que, cal remarcar, l'entitat imputada no ha desvirtuat, ni en la fase d'informació prèvia que precedí a aquest procediment sancionador, ni tampoc en el si d'aquest.

Per l'exposat, les al·legacions formulades per l'Ajuntament no poden reeixir.

3. En relació amb els fets descrits al punt 1r de l'apartat de fets provats, cal acudir a l'article 5.1 f) de l'RGPD, que regula el principi d'integritat i de confidencialitat, i determina que les dades personals han de ser "*tratados de tal manera que se garantiza una seguridad adecuada de los 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*".

Per la seva banda, l'article 32.1 de l'RGPD, referent a la seguretat de les dades, disposa el següent:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los 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 aplicaran 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 los datos personales de forma rápida en caso de incidente físico o técnico;*
- d. Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

A aquest respecte, la disposició addicional primera de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (en endavant, LOPDGDD) estableix el següent:

- “1. L’Esquema Nacional de Seguretat ha d’incloure les mesures que s’hagin d’implantar en cas de tractament de dades personals per evitar-ne la pèrdua, l’alteració o l’accés no autoritzat, amb l’adaptació dels criteris de determinació del risc en el tractament de les dades al que estableix l’article 32 del Reglament (UE) 2016/769.*
- 2. Els responsables que enumera l’article 77.1 d’aquesta Llei orgànica han d’aplicar als tractaments de dades personals les mesures de seguretat que corresponguin de les que preveu l’Esquema Nacional de Seguretat, així com impulsar un grau d’implementació de mesures equivalents en les empreses o fundacions subjectes al dret privat vinculades a aquells (...).”*

Els preceptes transcrits estableixen l’obligació del responsable del tractament, en aquest cas l’Ajuntament de (...), d’adoptar les mesures de seguretat apropiades per tal de garantir un nivell de seguretat adequat al risc.

Pel cas que aquí ens ocupa, cal tenir en compte les mesures de seguretat que preveia l’ENS, aprovat pel Reial Decret 3/2010, de 8 de gener, vigent en el moment de la comissió dels fets. En concret, els articles 13, 14.1, 16 i 23 del referit ENS, preveien el següent (el subratllat és nostre):

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 por medio del 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 todo caso, existirá una proporcionalidad entre ellas y los riesgos.*

Artículo 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 lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección e 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.

Així mateix, escau assenyalar que la Llei 26/2010, del 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya, a la seva disposició addicional onzena, sobre la gestió de la documentació i arxiu dels documents electrònics, estableix el següent:

“5. Els sistemes d'informació que utilitzin les administracions públiques incloses en l'àmbit d'aplicació d'aquesta llei han de garantir, sempre que sigui possible, l'autenticitat i la integritat de llurs dades, i també la traçabilitat de les accions que portin a terme”.

Durant la tramitació d'aquest procediment s'ha acreditat degudament el fet descrit al punt primer de l'apartat dels fets provats, consistent en la manca d'adopció de les mesures tècniques i de seguretat necessàries, que es considera constitutiu de la infracció prevista a l'article 83.4.a) l'RGPD, que tipifica la vulneració de “*las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 42*”, entre les quals hi ha la prevista a l'article 32.1 de l'RGPD.

La conducta que aquí s'aborda s'ha recollit com a infracció greu a l'article 73.f) de l'LOPDGDD, en la forma següent:

“La falta d'adopció de les mesures tècniques i organitzatives que siguin apropiades per garantir un nivell de seguretat adequat al risc del tractament, en els termes que exigeix l'article 32 del Reglament (UE) 2016/679.”

4. Pel que fa al fet descrit al punt 2n de l'apartat de fets provats, referent a la manca de realització d'un anàlisi de riscos, també cal acudir a l'article 5.1.f) de l'RGPD, transcrit al primer punt de la qualificació jurídica dels fets.

Al seu torn, l'apartat segon de l'article 32 de l'RGPD, en relació amb l'anàlisi de riscos, estableix el següent:

“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 dichos datos”.

També l'article 28 de l'LOPDGDD preveu l'obligació del responsable del tractament d'adoptar les mesures tècniques i organitzatives apropiades a fi de garantir i acreditar que el tractament és conforme a l'RGPD, tenint en compte, en particular, els riscos que es transcriuen tot seguit:

“2. Per a l'adopció de les mesures a què es refereix l'apartat anterior els responsables i encarregats del tractament han de tenir en compte, en particular, els riscos superiors que es poden produir en els supòsits següents:

a) Quan el tractament pugui generar situacions de discriminació, usurpació d'identitat o frau, pèrdues financeres, dany per a la reputació, pèrdua de confidencialitat de dades subjectes al secret professional, reversió no autoritzada de la pseudonimització o qualsevol altre perjudici econòmic, moral o social significatiu per als afectats.

b) Quan el tractament pugui privar els afectats dels seus drets i llibertats o els pugui impedir l'exercici del control sobre les seves dades personals.

- c) Quan es produeixi el tractament no merament incidental o accessori de les categories especials de dades a què es refereixen els articles 9 i 10 del Reglament (UE) 2016/679 i 9 i 10 d'aquesta Llei orgànica o de les dades relacionades amb la comissió d'infraccions administratives.
- d) Quan el tractament impliqui una avaluació d'aspectes personals dels afectats amb la finalitat de crear o utilitzar perfils personals d'aquests, en particular mitjançant l'anàlisi o la predicció d'aspectes referits al seu rendiment a la feina, la seva situació econòmica, la seva salut, les seves preferències o interessos personals, la seva fiabilitat o comportament, la seva solvència financera, la seva localització o els seus moviments.
- e) Quan es dugui a terme el tractament de dades de grups d'afectats en una situació d'especial vulnerabilitat i, en particular, de menors d'edat i persones amb discapacitat.
- f) Quan es produeixi un tractament massiu que impliqui un gran nombre d'afectats o comporti la recollida d'una gran quantitat de dades personals.
- g) Quan les dades personals hagin de ser objecte d'una transferència, amb caràcter habitual, a tercers estats o organitzacions internacionals respecte dels quals no s'hagi declarat un nivell adequat de protecció.
- h) Qualsevol altres que segons el parer del responsable o de l'encarregat puguin tenir rellevància i en particular els previstos en codis de conducta i estàndards definits per esquemes de certificació."

Doncs bé, en aquest cas, la manca d'anàlisi de riscos constitueix una infracció segons el previst a l'article 83.4 de l'RGPD que tipifica com a tal, la vulneració de "las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43", entre les quals hi ha la prevista a l'article 32.2 RGPD.

La infracció que aquí s'aborda s'ha recollit com a infracció greu a l'article 73.p) de l'LOPDGDD en la forma següent:

"p) El tractament de dades personals sense dur a terme una valoració prèvia dels elements que esmenta l'article 28 d'aquesta Llei orgànica."

5. Pel que fa a la conducta descrita al punt 3r dels fets imputats, referent a la divulgació del contingut d'una conversa telefònica, també cal acudir a l'article 5.1 f) de l'RGPD, transcrit al primer punt de la qualificació jurídica dels fets.

Per la seva banda, l'article 5 de l'LOPDGDD, relatiu al deure de confidencialitat, disposa:

- "1. Els responsables i encarregats del tractament de dades així com totes les persones que intervinguin en qualsevol fase d'aquest estan subjectes al deure de confidencialitat a què es refereix l'article 5.1. f) del Reglament (UE) 2016/679.*
- 2. L'obligació general que assenyala l'apartat anterior és complementària dels deures de secret professional de conformitat amb la seva normativa aplicable.*
- 3. Les obligacions que estableixen els apartats anteriors es mantenen encara que hagi finalitzat la relació de l'obligat amb el responsable o encarregat del tractament"*

Aquest fet imputat és constitutiu d'infracció, segons el previst a l'article 83.5 a) de l'RGPD, que tipifica com a tal, la vulneració dels "a) Los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5,6, 7 y 9", entre els quals hi ha el principi de confidencialitat.

Al seu torn, aquesta conducta s'ha recollit com a infracció molt greu a l'article 72.1 i) de l'LOPDGDD en la forma següent:

“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 substancial de los artículos mencionados en aquel y, en particular las siguientes: i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica”.

6. L'article 77.2 LOPDGDD disposa que, en el cas d'infraccions comeses pels responsables o encarregats enumerats a l'art. 77.1 LOPDGDD, l'autoritat de protecció de dades competent:

“(…) ha de dictar una resolució que les sancioni amb una amonestació. La resolució ha d'establir així mateix les mesures que escaigui adoptar perquè cessi la conducta o es corregeixin els efectes de la infracció que s'hagi comès.

La resolució s'ha de notificar al responsable o encarregat del tractament, a l'òrgan del qual depengui jeràrquicament, si s'escau, i als afectats que tinguin la condició d'interessat, si s'escau.”

En termes similars a l'LOPDGDD, l'article 21.2 de la Llei 32/2010, determina el següent:

“2. En el cas d'infraccions comeses amb relació a fitxers de titularitat pública, el director o directora de l'Autoritat Catalana de Protecció de Dades ha de dictar una resolució que declari la infracció i estableixi les mesures a adoptar per a corregir-ne els efectes. (...)”.

En virtut d'aquesta facultat, escau requerir l'Ajuntament de (...) perquè al més aviat possible, i en tot cas en el termini màxim de 10 dies a comptar des de l'endemà de la notificació d'aquesta resolució, implementi les mesures correctores que s'indiquen tot seguit:

6.1 Respecte els fets descrits al 1r punt de l'apartat de fets provats, acreditat disposar d'un registre d'accessos al sistema que emmagatzema les gravacions de les conversacions telefòniques mantingudes per la Policia Local.

6.2 Respecte els fets descrits al 2n punt de l'apartat de fets provats, documenti l'anàlisi de riscos referits als tractaments vinculats a l'enregistrament de les trucades telefòniques de la Policia Local i de les converses mantingudes a través dels equips de transmissions de l'Ajuntament.

Un cop s'hagin adoptat les mesures correctores descrites, en els terminis assenyalats, cal que en els 10 dies següents l'Ajuntament de (...) n'informi l'Autoritat, sense perjudici de la facultat d'inspecció d'aquesta Autoritat per fer les verificacions corresponents.

Respecte els fets descrits al 3r punt de l'apartat de fets provats, escau descartar l'adopció de mesures correctores atès que es tracta d'un fet puntual i consumat.

Per tot això, resolc:

1. Amonestar l'Ajuntament de (...) com a responsable de tres infraccions: dues infraccions previstes a l'article 83.4.a) en relació amb els apartats 1r i 2n de l'article 32, respectivament; i, una tercera infracció prevista a l'article 83.5.a) en relació amb l'article 5.1.f), tots ells de l'RGPD.
2. Requerir l'Ajuntament de (...) perquè adopti les mesures correctores assenyalades al fonament de dret 6è i acrediti davant d'aquesta Autoritat les actuacions dutes a terme per complir-les.
3. Notificar aquesta resolució a l'Ajuntament de (...).
4. Comunicar la resolució al Síndic de Greuges, de conformitat amb el que preveu l'article 77.5 de l'LOPDGDD.
5. Ordenar que es publiqui aquesta resolució al web de l'Autoritat (apdcat.gencat.cat), de conformitat amb l'article 17 de la Llei 32/2010, de l'1 d'octubre.

Contra aquesta resolució, que posa fi a la via administrativa d'acord amb els articles 26.2 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, i 14.3 del Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades, l'entitat imputada pot interposar, amb caràcter potestatiu, un recurs de reposició davant la directora de l'Autoritat Catalana de Protecció de Dades, en el termini d'un mes a comptar des de l'endemà de la seva notificació, d'acord amb el que preveuen l'article 123 i següents de l'LPAC. També pot interposar directament un recurs contenciós administratiu davant els jutjats contenciosos administratius, en el termini de dos mesos a comptar des de l'endemà de la seva notificació, d'acord amb els articles 8, 14 i 46 de la Llei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa administrativa.

Si l'entitat imputada manifesta a l'Autoritat la seva intenció d'interposar un recurs contenciós administratiu contra la resolució ferma en via administrativa, la resolució se suspendrà cautelarment en els termes previstos a l'article 90.3 de l'LPAC.

Igualment, l'entitat imputada pot interposar qualsevol altre recurs que consideri convenient per defensar els seus interessos.

La directora,