Dictamen en relació amb la consulta formulada per una empresa pública sobre el nivell de seguretat a aplicar a un tractament de dades personals del que n'és responsable

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit emès per una empresa municipal, en què se sol·licita el parer de l'Autoritat sobre el nivell de seguretat que ha d'aplicar aquesta empresa a un determinat tractament de dades personals.

Analitzada la consulta, i vist l'informe de l'Assessoria Jurídica, es dictamina el següent:

I

(...)

II

L'empresa municipal manifesta, en el seu escrit de consulta, que utilitza, com a eina de gestió d'actius multimèdia, el programari DALET, format per un conjunt d'aplicacions que permeten gravar, programar, editar i arxivar les notícies i els programes que formen part del contingut de ràdio.

Aquest programari permet mantenir un arxiu històric amb les entrevistes o declaracions realitzades per a aquests programes de ràdio, de manera intacte o editades, durant un període de temps concret, d'acord amb allò establert a la Llei 22/2005, de 29 de desembre, de la comunicació audiovisual de Catalunya.

En la mesura que aquest material es pot mantenir arxivat en una base de dades, l'ús d'aquest programari també permetrà, com bé apunta l'empresa en el seu escrit, mantenir emmagatzemades determinades dades de caràcter personal de les persones que han participat en aquests programes. En aquest sentit, s'assenyala que s'emmagatzema informació acústica (veu) referent a persones físiques identificades o identificables que consenten la seva gravació i que, a més a més, també és possible desar-hi informació de qualsevol tipus, com ara, dades relatives a la ideologia, afiliació sindical, vida sexual, etc.

És, precisament, en relació amb el tractament d'aquesta informació personal que l'empresa municipal planteja a aquesta Autoritat quin nivell de mesures de seguretat li correspon aplicar, tenint en compte aspectes com el caràcter públic de les declaracions, el dret d'accés a la informació i el fet que el tractament el du a terme un mitjà de comunicació.

L'anàlisi d'aquesta qüestió es realitza en el següent apartat d'aquest dictamen.

III

La Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, LOPD) defineix, en el seu article 3.a), les dades de caràcter personal com *"qualsevol informació referent a persones físiques identificades o identificables"*.

Afegeix l'article 5.1.f) del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la LOPD (en endavant, RLOPD) que dada de caràcter personal és *"qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus que concerneix persones físiques identificades o identificables".* Es considera que una persona és identificable quan la seva identitat "*es pugui determinar, directament o indirectament, mitjançant qualsevol informació referida a la seva identitat física, fisiològica, psíquica, econòmica, cultural o social. Una persona física no es considera identificable si la dita identificació requereix terminis o activitats desproporcionats"* (article 5.1.o) RLOPD).

En el cas examinat, com s'ha avançat, el programari DALET de gestió d'actius multimèdia permet gravar, editar i/o arxivar les entrevistes o declaracions realitzades per les persones físiques que participen en els programes radiofònics de ràdio, fet que comporta també la captació, l'enregistrament i l'emmagatzematge d'informació personal, principalment, de la veu, així com d'altres dades personals que en el si d'aquestes entrevistes i/o declaracions puguin revelar-se. Per tant, el tractament d'aquesta informació (article 3.c) LOPD), que conté dades personals, per part de l'empresa municipal (la responsable), estarà subjecte als principis i obligacions de la normativa en matèria de protecció de dades.

En aquest sentit, convé tenir en compte, als efectes que interessen en aquest dictamen, que la normativa de protecció de dades personals imposa l'obligació al responsable del tractament i, si s'escau, a l'encarregat del tractament d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries per tal de garantir la seguretat de les dades personals que seran tractades, així com per evitar la seva alteració, pèrdua, tractament o accés no autoritzat (article 9 LOPD).

Aquestes mesures de seguretat venen regulades en el Títol VIII del RLOPD, que les classifica en tres nivells diferents –bàsic, mitjà i alt- en funció de la tipologia de dades personals que en cada cas es prevegin tractar. Cal tenir en compte, que aquestes mesures tenen un caràcter acumulatiu, de tal manera que les establertes per a cada nivell exigeixen incorporar les previstes per als nivells inferiors.

L'article 81 del RLOPD estableix, en relació amb l'aplicació dels nivells de seguretat, el següent:

> *"1. Tots els fitxers o tractaments de dades de caràcter personal han d'adoptar les mesures de seguretat qualificades de nivell bàsic.*
> *2. S'han d'implantar, a més de les mesures de seguretat de nivell bàsic, les mesures de nivell mitjà, en els següents fitxers o tractaments de dades de caràcter personal:*
> *a) Els relatius a la comissió d'infraccions administratives o penals.*
> *b) Aquells el funcionament dels quals es regeixi per l'article 29 de la Llei orgànica 15/1999, de 13 de desembre.*
> *c) Aquells els responsables dels quals siguin administracions tributàries i es relacionin amb l'exercici de les seves potestats tributàries.*
> *d) Aquells els responsables dels quals siguin les entitats financeres per a finalitats relacionades amb la prestació de serveis financers.*
> *e) Aquells els responsables dels quals siguin les entitats gestores i serveis comuns de la Seguretat Social i es relacionin amb l'exercici de les seves competències. De la mateixa manera, aquells els responsables dels quals siguin les mútues d'accidents de treball i malalties professionals de la Seguretat Social.*

f) Els que continguin un conjunt de dades de caràcter personal que ofereixin una definició de les característiques o de la personalitat dels ciutadans i que permetin avaluar determinats aspectes de la seva personalitat o comportament.
3. A més de les mesures de nivell bàsic i mitjà, les mesures de nivell alt s'han d'aplicar en els següents fitxers o tractaments de dades de caràcter personal:
a) Els que es refereixin a dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual.
b) Els que continguin o es refereixin a dades obtingudes per a fins policials sense consentiment de les persones afectades.
c) Els que continguin dades derivades d'actes de violència de gènere.
4. Als fitxers els responsables dels quals siguin els operadors que prestin serveis de comunicacions electròniques disponibles al públic o explotin xarxes públiques de comunicacions electròniques respecte a les dades de tràfic i a les dades de localització, s'hi han d'aplicar, a més de les mesures de seguretat de nivell bàsic i mitjà, la mesura de seguretat de nivell alt que conté l'article 103 d'aquest Reglament.
5. En el cas de fitxers o tractaments de dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual només s'han d'implantar les mesures de seguretat de nivell bàsic quan:
a) Les dades s'utilitzin amb l'única finalitat de realitzar una transferència dinerària a les entitats de què els afectats siguin associats o membres.
b) Es tracti de fitxers o tractaments on de forma incidental o accessòria s'incloguin aquelles dades sense tenir relació amb la seva finalitat. 6
6. També es poden implantar les mesures de seguretat de nivell bàsic en els fitxers o tractaments que continguin dades relatives a la salut, referents exclusivament al grau de discapacitat o la simple declaració de la condició de discapacitat o invalidesa de l'afectat, amb motiu del compliment de deures públics.
7. Les mesures incloses en cadascun dels nivells descrits anteriorment tenen la condició de mínims exigibles, sense perjudici de les disposicions legals o reglamentàries específiques vigents que puguin ser aplicables en cada cas o les que per pròpia iniciativa adopti el responsable del fitxer.
8. Als efectes de facilitar el compliment del que disposa aquest títol, quan en un sistema d'informació existeixin fitxers o tractaments que, en funció de la seva finalitat o ús concret, o de la naturalesa de les dades que continguin, requereixin l'aplicació d'un nivell de mesures de seguretat diferent que el del sistema principal, es poden segregar d'aquest últim, i és aplicable en cada cas el nivell de mesures de seguretat corresponent i sempre que es puguin delimitar les dades afectades i els usuaris que hi tinguin accés, i que això es faci constar en el document de seguretat."

D'acord amb aquest precepte, atès que, en aquest cas, a banda de l'enregistrament i l'emmagatzematge de la veu dels participants en els programes de ràdio (dada personal de caràcter identificatiu), és possible que també siguin enregistrades i emmagatzemades altre tipus d'informacions de caràcter més sensible, com ara, a tall d'exemple, ideologia, afiliació sindical, vida sexual, etc., les mesures de seguretat que ha d'implementar l'empresa pública, com a responsable d'aquest tractament, són, a més de les mesures de nivell bàsic i mitjà, les mesures de nivell alt (article 81.3.a) RLOPD).

En aquest punt, convé assenyalar que la normativa de protecció de dades atorga una protecció reforçada a aquest tipus d'informacions més sensible, considerades dades especialment protegides (article 7 LOPD), ateses les conseqüències negatives que del

seu tractament se'n poden derivar per la persona que n'és titular. Així, si amb caràcter general, qualsevol tractament de dades (com, per exemple, la veu) exigeix comptar amb el consentiment inequívoc de l'afectat, llevat que una llei disposi una altra cosa (article 6.1 LOPD), en el cas de les dades especialment protegides el consentiment atorgat per les persones afectades ha de ser exprés, quan es prevegi tractar dades que es refereixen a l'origen racial, a la salut i a la vida sexual, tret que una llei, per motius d'interès general, ho permeti (article 7.3 LOPD), i/o exprés i per escrit, quan es prevegi tractar dades que revelen la ideologia, la religió, les creences o l'afiliació sindical (article 7.2 LOPD).

Dit això, tenint en compte que el tractament de dades s'efectua de manera automatitzada, en aquest cas correspon aplicar les mesures descrites en els articles 89 a 104 del RLOPD, consistents en:

a) L'elaboració d'un document de seguretat on es fixin les obligacions i funcions dels usuaris o perfils d'usuaris que accedeixin a les dades, una descripció del sistema informàtic i una definició de les funcions de control o autoritzacions delegades pel responsable del fitxer o tractament (article 89 RLOPD).
b) L'establiment d'un registre d'incidències (articles 90 i 100 RLOPD).
c) L'establiment d'un control d'accés (article 91 RLOPD).
d) La correcta gestió de suports i documents (articles 92, 97 i 101 RLOPD).
e) L'adopció de mesures que garanteixin la correcta identificació i autenticació dels usuaris (articles 93 i 98 RLOPD).
f) L'establiment de processos de còpies de seguretat i recuperació de les dades (articles 94 i 102 RLOPD).
g) L'assignació d'un o diversos responsables de seguretat (article 95 RLOPD).
h) La realització d'auditories de seguretat (article 96 RLOPD).
i) L'establiment d'un control d'accés físic (article 99 RLOPD).
j) L'establiment d'un registre d'accessos (article 103 RLOPD).
k) L'establiment de mecanismes de xifratge, en cas de transmissió de les dades a través de xarxes públiques o xarxes sense fil de comunicacions electròniques (article 104 RLOPD).

Cal insistir en què la implementació d'aquestes mesures de seguretat és obligatòria per al responsable del fitxer o tractament i, si escau, per a l'encarregat del tractament (article 9 LOPD), amb independència del fet que la persona afectada hagi donat el consentiment per al tractament de les seves dades o de quina sigui la naturalesa del responsable del fitxer o tractament. Aspectes com els assenyalats per l'empresa municipal en el seu escrit de consulta, tals com el caràcter públic de les declaracions, el dret d'accés a la informació i el fet que el tractament el dugui a terme un mitjà de comunicació, no alteren l'obligatorietat de la seva implementació.

L'aplicació de les mesures de seguretat ve determinada per la tipologia de la informació tractada. Per tant, tret d'algunes excepcions previstes en el mateix article 81 del RLOPD i que no són aplicables en aquest cas, quan es tractin dades que requereixen l'aplicació de mesures de seguretat de nivell alt, caldrà aplicar necessàriament aquest nivell.

Convé destacar la importància de la seva adopció, atès que l'objectiu perseguit amb la seva implementació és garantir no només la confidencialitat, sinó també la integritat i la disponibilitat de la informació amb la finalitat de garantir el dret fonamental a la protecció de dades personals.

En aquest sentit, convé recordar que, de conformitat amb allò disposat a l'article 44.3.h) de la LOPD, constitueix infracció greu *"mantenir els fitxers, locals, programes o*

equips que continguin dades de caràcter personal sense les degudes condicions de seguretat que es determinin per via reglamentària".

D'acord amb les consideracions fetes en aquest dictamen en relació amb la consulta plantejada, es fan les següents,

Conclusions

D'acord amb la normativa vigent en matèria de protecció de dades personals, el responsable del tractament i, si s'escau, l'encarregat del tractament han d'adoptar les mesures de caràcter tècnic i organitzatiu que siguin necessàries per tal de garantir la seguretat de les dades personals tractades, així com per evitar la seva alteració, pèrdua, tractament o accés no autoritzat (article 9 LOPD).

En el cas examinat, el tractament de dades personals especialment protegides, mitjançant l'ús del programari DALET, obliga a l'empresa municipal, com a responsable d'aquest tractament, a implementar, a més de les mesures de seguretat de nivell bàsic i mitjà, les de nivell alt (article 81.3.a) RLOPD).

Barcelona, 17 de febrer de 2012