CNS 48/2016

Dictamen en relació amb la consulta d'un Ajuntament sobre l'ús de dispositius GPS en els vehicles policials.

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'un Ajuntament en el qual demana que l'Autoritat emeti un dictamen sobre l'ús de dispositius GPS en els vehicles policials de l'Ajuntament.

En concret, la consulta planteja si, des del punt de vista de la protecció de dades, l'ús de dispositius GPS en els vehicles policials vulnera algun dret dels treballadors i si cal seguir algun procediment per legalitzar els dispositius.

Analitzada la petició, que no s'acompanya de cap altre document, i la normativa vigent aplicable i, d'acord amb l'informe de l'Assessoria Jurídica, emeto el dictamen següent:

I

(...)

II

En primer lloc, és necessari determinar si la instal·lació d'un sistema de geolocalització com el que planteja la consulta suposa el tractament de dades personals.

La Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD) defineix com a dada personal *"qualsevol informació referent a persones físiques identificades o identificables"* (article 3 LOPD). Segons l'article 5.1.f) del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de l'LOPD (RLOPD), és dada de caràcter personal *"qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus que concerneix persones físiques identificades o identificables".*

En aquest sentit, l'RLOPD concreta que és identificable *"qualsevol persona la identitat de la qual 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 aquesta identificació requereix terminis o activitats desproporcionats*" (article 5.1.o).

En el cas que ens ocupa, si bé les dades de geolocalització per si soles permetrien localitzar un objecte –el vehicle policial– i no una persona, en la mesura que aquesta informació es pot combinar o associar fàcilment amb altres dades de les que disposa l'Ajuntament, semblaria que la identificació dels agents és possible sense esforços desproporcionats i, per tant, estaríem en presència de dades personals.

Així mateix, s'entén per tractament de dades "*les operacions i els procediments tècnics de caràcter automatitzat o no, que permetin recollir, gravar, conservar, elaborar, modificar, bloquejar i cancel·lar, així com les cessions de dades que derivin de comunicacions, consultes, interconnexions i transferències*" (article 3.c) LOPD).

D'acord amb aquests preceptes, per tant, la utilització d'un sistema de geolocalització que permeti la identificació de persones físiques, en aquest cas a través de l'associació entre el cotxe policial i els agents que l'utilitzen, comportaria un tractament de dades que es trobaria subjecte al compliment dels principis i garanties de la normativa de protecció de dades.

III

L'article 6.1 de l'LOPD estableix, amb caràcter general, que *"el tractament de les dades de caràcter personal requereix el consentiment inequívoc de l'afectat, llevat que la llei disposi una altra cosa*". No obstant això, l'article 6.2 afegeix que el consentiment dels afectats no és necessari en diversos supòsits, entre d'altres per a *"l'exercici de les funcions pròpies de les administracions públiques en l'àmbit de les seves competències".*

Tot i que la consulta no determina quina és la finalitat del tractament, si aquesta fos l'adequada prestació del servei policial, el tractament de les dades de localització dels cotxes patrulla i, per tant, dels policies que els ocupen, vindria emparat en l'article 6.2 de l'LOPD i el consentiment dels interessats no seria preceptiu.

Referent a aquesta qüestió, resulta d'interès fer esment del document elaborat per aquesta Autoritat relatiu a "*La protecció de dades de caràcter personal en les ciutats intel·ligents (Smart Cities)"*, que està disponible al lloc web www.apd.cat. En aquest document s'apunta que:

"L'article 6 de la LOPD configura el consentiment inequívoc del titular de les dades com l'eix que legitima un tractament de dades, llevat que la llei disposi una altra cosa, en definitiva, que es donin les circumstàncies legals que habiliten un tractament de dades sense haver de disposar del consentiment. Especialment, caldrà tenir en compte les previsions sobre diferents tipus de consentiment requerit, en funció de la informació personal tractada (art. 7 LOPD). Ara bé, tractant-se d'administracions públiques, que tenen encomanda per lleis la consecució de l'interès públic, la mateixa LOPD habilita el tractament quan es tracti de "l'exercici de les funcions pròpies de les administracions públiques en l'àmbit de les seves competències" (art. 6.2).

En el context de les Smart City, podem trobar molts exemples i iniciatives que es duen a terme des del sector públic. En aquests casos, quan una Administració pública recull dades personals dels ciutadans per tractar-les en el context de l'exercici de les funcions que li són pròpies, caldria partir de la base que no seria necessari disposar del consentiment previ de l'afectat. El tractament pot ser legítim sense el consentiment previ dels afectats.

A tall d'exemple, citem la instal·lació de sistemes de geolocalització en vehicles de cossos policials, en serveis d'emergència (bombers...) o serveis de transport públic, com ara els autobusos o els taxis que circulen per una ciutat. En aquests casos, sempre que la instal·lació trobi la seva justificació en l'adequada prestació del propi servei (en el sentit que conèixer la situació i recorreguts de la flota de vehicles

suposa la millora del propi servei –reducció de temps d'espera en víctimes d'accidents, millora en els temps d'atenció de trucades d'emergència...-, o bé perquè augmenta la seguretat dels propis treballadors i de terceres persones, etc.), podria resultar legítima una recollida i tractament de les dades sense consentiment. Per contra, altres supòsits d'utilització de la geolocalització a través de dispositius mòbils intel·ligents (com ara smartphones) o a través de targetes intel·ligents, de forma generalitzada per als usuaris d'un serveis públic, que sigui "prescindible", és a dir, no justificable en la pròpia prestació del servei o en l'exercici de la funció pròpia de l'Administració pública, podria requerir el consentiment previ dels afectats."

Dit això, cal partir de la base que l'establiment de la relació laboral no té perquè justificar el seguiment dels treballadors fora del centre de treball. No obstant això, pot haver-hi determinats serveis o funcions que ho poden requerir i, en aquest sentit, sembla raonable que qui té el comandament de la policia local hagi de saber on estan situats els vehicles policials en cada moment per tal de, per exemple, enviar el vehicle que es troba més a prop del lloc on es requereix la presència policial. D'acord amb això, en el cas que ens ocupa, si el tractament de les dades de geolocalització es du a terme per assegurar el normal funcionament del servei, l'Ajuntament no necessitaria disposar del consentiment previ dels afectats.

Ara bé, en el cas que ens ocupa, el correcte funcionament del servei pot justificar únicament el tractament de les dades que siguin estrictament necessàries per assolir aquesta finalitat. En aquest sentit resulta d'interès el Dictamen 13/2011 del Grup de Treball de l'Article 29, sobre els serveis de geolocalització en els dispositius mòbils intel·ligents, que sosté que *"el empresario debe siempre buscar los medios menos intrusivos, evitar un seguimiento continuo y, por ejemplo, elegir un sistema que envíe una alerta cuando un empleado cruce una frontera virtual preestablecida. El empleado deberá poder desactivar cualquier dispositivo de vigilancia fuera de las horas de trabajo y deberá instruírsele sobre cómo hacerlo. Los dispositivos de seguimiento de vehículos no son dispositivos para la localización de empleados ya que su función es hacer un seguimiento o vigilar la ubicación de los vehículos en que estén instalados. Los empresarios no deben considerarlos como dispositivos para seguir o supervisar el comportamiento o el paradero de los conductores o de otro tipo de personal, por ejemplo, mediante el envío de alertas relacionadas con la velocidad del vehículo".*

Per tant, d'acord amb el principi de qualitat (art. 4 LOPD), el tractament de dades personals ha de ser el mínim indispensable per poder donar compliment a la finalitat del tractament i, per tant, s'haurà de limitar a les dades que siguin estrictament necessàries, pertinents i adequades per donar compliment a la finalitat pretesa. A més, les dades s'hauran de destinar a la finalitat determinada, explícita i legítima per a la qual es van recollir i, per tant, serà contrari a aquest principi qualsevol ús que se'n faci destinat a una finalitat incompatible amb aquella que va motivar-ne la recollida. Pel que fa a la seva conservació, les dades s'hauran de cancel·lar quan no siguin necessàries o pertinents per assolir la finalitat perseguida. No obstant això, les dades cancel·lades s'hauran de conservar a disposició de les administracions públiques, jutges i tribunals degudament bloquejades durant el temps en què es pugui exigir algun tipus de responsabilitat.

IV

Quant al deure d'informar, s'ha de recordar que, amb independència que pugui operar l'excepció de l'article 6.2 de l'LOPD, que habilitaria el tractament de les dades sense

consentiment previ dels afectats, la concurrència d'aquesta excepció no eximeix l'Ajuntament d'informar degudament els afectats sobre el tractament de les seves dades. En concret, l'article 5.1 de l'LOPD configura aquest deure en els termes següents:

"1. Els interessats als quals se sol·licitin dades personals han de ser prèviament informats de manera expressa, precisa i inequívoca:
a) De l'existència d'un fitxer o un tractament de dades de caràcter personal, de la finalitat de la recollida de les dades i dels destinataris de la informació.
b) Del caràcter obligatori o facultatiu de la resposta a les preguntes que els siguin plantejades.
c) De les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.
d) De la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.
e) De la identitat i la direcció del responsable del tractament o, si s'escau, del seu representant.
(...)"

La Sentència del Tribunal Constitucional 292/2000, de 30 de novembre, en delimitar el contingut del dret fonamental a la protecció de dades personals, ha considerat el dret d'informació de l'afectat com un element essencial del contingut del dret fonamental en declarar que *"el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.*

Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele".

D'acord amb això, l'Ajuntament haurà de donar compliment al deure d'informació als interessats de manera expressa, precisa i inequívoca, respecte dels extrems que preveu l'article 5 de l'LOPD, a través d'un mitjà que permeti acreditar-ne el compliment i que haurà de conservar mentre persisteixi el tractament (art. 18 RLOPD). Per altra banda, donat que aquesta mesura afecta bona part de la plantilla, també serà necessari fer extensiva aquesta informació als representants dels treballadors (art. 40.1

Reial Decret Legislatiu 5/2015, de 30 d'octubre, pel qual s'aprova el text refós de la Llei de l'Estatut Bàsic de l'Empleat Públic).

Dit això, s'ha de fer notar que el nou Reglament General de Protecció de Dades 2016/679, de 27 d'abril del Parlament Europeu i del Consell (RGPD), amplia la informació que s'ha de facilitar als afectats, incorporant nous aspectes sobre els que cal informar. Atès que l'article 99.2 estableix que el Reglament General de Protecció de Dades no serà aplicable fins el 25 de maig de 2018, segueix vigent fins aquella data el règim previst a l'LOPD i a l'RLOPD, però cal tenir present que, a partir de la data esmentada, el nou Reglament comporta, entre d'altres, haver d'informar respecte dels extrems següents que siguin d'aplicació al cas concret (article 13 RGPD): les dades de contacte del delegat de protecció de dades; la base jurídica del tractament; els interessos legítims perseguits en què es fonamenti el tractament; la intenció de transferir les dades a un país tercer o organització internacional i la base per a fer-ho; el termini durant el qual es conservaran les dades; l'existència del dret a demanar la portabilitat; el dret a retirar en qualsevol moment el consentiment que s'hagi prestat; si la comunicació de dades és un requisit legal o contractual o un requisit necessari per subscriure un contracte; el dret a presentar una reclamació davant una autoritat de control; l'existència de decisions automatitzades, incloent la lògica aplicada i les seves conseqüències. Tot i que, com s'ha dit, la informació relativa a aquests nous aspectes no és exigible fins el mes de maig de 2018, es recomana –sempre que sigui possible– incorporar-la des d'ara a la informació facilitada als interessats.

V

Pel que fa a la segona pregunta que es formula a la consulta, més enllà de la necessitat de donar compliment al deure d'informar els interessats sobre el tractament de les seves dades personals, és necessari recordar que l'Ajuntament, amb l'aprovació prèvia de la preceptiva disposició general, haurà de crear el fitxer corresponent (o modificar-ne un d'existent) i notificar-ho a aquesta Autoritat, per preveure la recollida de les dades de geolocalització a l'estructura del fitxer i així tenir cobertura per tractar les dades personals recopilades a través del sistema GPS.

A aquest respecte, l'article 20 de l'LOPD preveu que:

"1. La creació, la modificació o la supressió dels fitxers de les administracions publiques només es poden fer per mitjà d'una disposició general publicada en el Butlletí Oficial de l'Estat o en el diari oficial corresponent.
2. Les disposicions de creació o de modificació de fitxers han d'indicar:
a) La finalitat del fitxer i els usos previstos.
b) Les persones o els col·lectius sobre els quals es pretén obtenir dades de caràcter personal o que estiguin obligats a subministrar-les.
c) El procediment de recollida de les dades de caràcter personal.
d) L'estructura bàsica del fitxer i la descripció dels tipus de dades de caràcter personal incloses en el mateix fitxer.
e) Les cessions de dades de caràcter personal i, si s'escau, les transferències de dades que es prevegin a països tercers.
f) Els òrgans de les administracions responsables del fitxer.
g) Els serveis o les unitats davant els quals es puguin exercir els drets d'accés, rectificació, cancel·lació i oposició.
h) Les mesures de seguretat amb indicació del nivell bàsic, mitjà o alt exigible.
3. En les disposicions que es dictin per a la supressió dels fitxers, se n'ha d'establir el destí o, si s'escau, les previsions que s'adoptin per destruir-los."

Cal afegir, en resposta a una de les preguntes plantejades per la consulta, que les dades de geolocalització obtingudes mitjançant els diferents dispositius GPS per a una mateixa finalitat poden formar part d'un sol fitxer, sense que sigui necessària la creació d'un fitxer per cada dispositiu GPS.

Pel que fa a la necessitat de creació de fitxers i a la seva notificació al Registre de protecció de dades, s'ha de fer notar que el nou Reglament General de Protecció de Dades 2016/679, de 27 d'abril del Parlament Europeu i del Consell, ha suprimit la seva exigibilitat. Però cal tenir en compte que, atès que –com s'ha dit– l'article 99.2 estableix que el Reglament no serà aplicable fins el 25 de maig de 2018, segueix vigent fins aquesta data l'obligació de crear i notificar el fitxer, d'acord amb l'article 20 de l'LOPD.

Més enllà d'aquest deure de creació i notificació dels fitxers, la normativa vigent de protecció de dades no conté cap previsió que exigeixi cap procediment de legalització dels dispositius.

D'acord amb aquestes consideracions, es fan les següents,

Conclusions,

L'ús de dispositius GPS en els vehicles policials comporta el tractament de dades personals i, per tant, està sotmès a la normativa de protecció de dades personals.

Si el tractament es du a terme per assegurar el normal funcionament del servei, l'Ajuntament no necessitaria disposar del consentiment previ dels afectats, però sí que hauria de complir el deure d'informació i l'obligació de creació (o modificació) i notificació del fitxer que contingui les dades de geolocalització.

Barcelona, 16 de setembre de 2016