CNS 43/2020

Dictamen en relació amb la consulta formulada per un ajuntament sobre la creació d'una xarxa supramunicipal per a l'intercanvi d'informació policial

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit del delegat de protecció de dades d'un ajuntament en el qual es demana que l'Autoritat emeti un dictamen sobre la creació d'una xarxa supramunicipal per a l'intercanvi d'informació policial.

Analitzada la petició, i vist l'informe de l'Assessoria Jurídica, es dictamina el següent.

I

(...)

II

L'Ajuntament exposa en la seva consulta que és del seu interès crear una xarxa entre les corporacions locals que utilitzen el mateix programa informàtic de gestió policial per compartir, entre cossos policials, la informació registrada en aquest programa arran les actuacions efectuades per la policia local.

Tot seguit, detalla els aspectes següents d'aquest sistema d'informació:

1. En accedir al sistema caldrà indicar obligatòriament el motiu de la consulta:

- Requeriment/suport judicial.
- Prevenció i seguretat ciutadana.

2. Per a cada accés s'enregistrarà la identificació de l'usuari, la data i l'hora en què es realitza l'accés, les dades consultades i el motiu de la consulta.

3. La informació a consultar/intercanviar del sistema serà la següent:

- Persones físiques: nom i cognoms; núm. DNI/NIE/Passaport o document estranger; sexe; data de naixement; lloc de naixement; nacionalitat; data de defunció (si fos el cas); àlies; nom del pare i la mare; domicili/s; telèfon/s; correu/s electrònic/s; data creació/modificació del registre; mòdul del programa de gestió amb què està relacionada la persona (novetat diària, accident de trànsit, atestat, citació judicial, etc.).

- Persones jurídiques: nom comercial; CIF; activitat; domicili/s; telèfon/s; correu/s electrònic/s; dades persona/es de contacte; data creació/modificació del registre; mòdul del programa de gestió amb què està relacionada l'entitat o empresa.

- Vehicles: matrícula; marca; model; bastidor; tipus de vehicle; assegurança; dades de la persona propietària; mòdul del programa de gestió amb què està relacionat.

- Tinença d'animals: microxip; tipus microxip; nom de l'animal; espècie animal; raça; perillositat; data naixement; data de defunció (si fos el cas); dades de la persona propietària.

L'Ajuntament manifesta que té formalitzat amb l'empresa propietària del programa informàtic de gestió policial el corresponent contracte d'encarregat del tractament. També que s'està duent a terme una anàlisi de riscos i que es preveu, si s'escau, la realització d'una avaluació d'impacte.

A tot això, planteja si el sistema d'accés, consulta i intercanvi d'informació per a les corporacions locals que s'adherissin voluntàriament a aquest sistema d'informació policial, en els termes exposats, compleix amb la normativa vigent sobre protecció de dades personals.

III

Per tal de donar resposta a la consulta efectuada, cal analitzar, d'entrada, quina seria la normativa de protecció de dades aplicable.

El Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (RGPD), no resulta aplicable als tractaments que es duen a terme en l'àmbit policial i judicial penal, segons es desprèn de l'article 2.2.d) de l'RGPD, que disposa el següent:

> *"2. El presente Reglamento no se aplica al tratamiento de datos personales:*
> *(...)*
> *d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención."*

En aquest àmbit cal tenir en consideració la Directiva (UE) 2016/680 del Parlament i del Consell, de 27 d'abril de 2016, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les autoritats competents per a finalitats de prevenció, recerca, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals, i a la lliure circulació d'aquestes dades i per la qual es deroga la Decisió marc 2008/977/JAI del Consell.

Els estats membres de la Unió Europea havien de transposar la Directiva (UE) 2016/680 abans del 6 de maig de 2018.

Atesa la manca de transposició d'aquesta Directiva per part d'Espanya, en el cas que ens ocupa cal tenir en compte les previsions de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGGD), que a la disposició transitòria quarta estableix el següent:

> *"Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo,* ***continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo****, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva."*

Per tant, en aquest cas cal tenir present les previsions de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD) i les disposicions que la despleguen.

IV

En la consulta es planteja la possible creació d'un sistema supramunicipal d'informació policial que permeti al cos policial de les corporacions locals que s'hi adhereixin voluntàriament consultar i, per tant, intercanviar informació d'interès policial.

En aquest sistema, per la informació de què es disposa, s'incorporarà la informació de què disposa cada policia local com a conseqüència de l'exercici de les seves funcions (tant arran de serveis planificats, com a requeriment dels ciutadans), la qual inclou dades personals, i que el cos policial gestiona a través d'un programa informàtic anomenat DRAG, creat per una empresa privada.

Més enllà d'això, en la consulta no queda clar el paper dels diferents agents implicats en aquest sistema d'informació. En qualsevol cas, i a manca d'informació més precisa sobre el model que es vol adoptar, la finalitat pretesa es podria assolir a través de diversos models organitzatius alternatius.

D'acord amb l'article 3.d) de l'LOPD, s'entén per "responsable del fitxer o tractament" la *"persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".*

En la consulta s'apunta que l'Ajuntament *"té interès en crear una xarxa entre les corporacions locals que utilitzen el mateix programa DRAG"*, manifestació de la qual podria desprendre's que aquesta corporació local assumeix la posició de responsable del sistema d'informació i, per tant, de responsable del tractament.

Tampoc es podria descartar però que ens trobéssim davant un supòsit de corresponsabilitat, això és que les diferents corporacions locals que disposen d'aquest programa informàtic de gestió d'informació policial (DRAG) acordin i participin conjuntament en la creació del nou sistema d'informació policial, per tant, en la definició dels fins i mitjans del tractament.

Per bé que el terme de corresponsables del tractament no es troba definit expressament a l'LOPD, sí que s'hi refereix l'article 5.1.q) del Reglament de desplegament de l'LOPD, aprovat pel Reial decret 1720/2007, de 21 de desembre (RLOPD), en definir el responsable del tractament com la "*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, **que sólo o conjuntamente con otros** decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente*.".

En qualsevol cas, aquesta figura sí es troba recollida en la Directiva 2016/680, que ha d'ésser objecte de transposició a l'ordenament jurídic espanyol.

L'article 21 de la Directiva disposa que:

> *"1. Los Estados miembros dispondrán que, **cuando dos o más responsables del tratamiento determinen conjuntamente los objetivos y los medios de tratamiento, sean considerados corresponsables del tratamiento**. Determinarán, de modo transparente y de mutuo acuerdo, cuáles serán sus responsabilidades respectivas en el cumplimiento de la presente Directiva, en particular por lo que se refiere al ejercicio de los derechos del interesado y a sus respectivas obligaciones en el suministro de la*

información contemplada en el artículo 13, salvo y en la medida en que las responsabilidades respectivas de los responsables se rijan por el Derecho de la Unión o del Estado miembro a que estén sujetos los responsables del tratamiento. El citado acuerdo designará el punto de contacto para los interesados. Los Estados miembros podrán designar cuál de los corresponsables puede actuar como punto único de contacto para el interesado por lo que respecta al ejercicio de sus derechos.
2. Independientemente de los términos del acuerdo a que hace referencia el apartado 1, los Estados miembros podrán disponer que el interesado pueda ejercer los derechos que le reconocen las disposiciones adoptadas con arreglo a la presente Directiva con respecto a cada uno de los responsables y frente a ello."

Per tant, de tractar-se el present cas d'un supòsit de corresponsabilitat, seria convenient tenir en compte el que s'estableix en aquest precepte, sens perjudici del que pugui establir-se en la futura norma de transposició.

Sigui com sigui, advertir que la responsabilitat en aquests casos abastaria només a la informació policial incorporada al nou sistema d'informació, no així a la informació de què disposa cada corporació local en els respectius sistemes d'informació de gestió policial. En aquest cas, cada policia local seria responsable del tractament de la informació generada per les seves actuacions, sens perjudici que, un cop incorporada al nou sistema, passi a formar part de la responsabilitat de l'Ajuntament consultant (o, si fos el cas, del conjunt d'ens locals participants (cas de corresponsables)).

Pel que fa a l'empresa creadora del programa informàtic de gestió policial DRAG, en la consulta s'assenyala que es compta amb el corresponent contracte d'encàrrec del tractament, el qual comprèn *"clàusules contractuals amb els continguts generals del règim jurídic de l'encàrrec i els continguts específics d'aquest tipus d'encàrrec del tractament".*

Per tant, la dita empresa ostentaria en el present cas la condició d'encarregada del tractament (article 3.g) LOPD), entesa com *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".*

Més enllà que aquest contracte d'encàrrec del tractament hagi d'adequar-se a les previsions de l'article 12 de l'LOPD, mentre no entri en vigor la norma que transposi al dret espanyol la Directiva 2016/680, es recomana tenir també en compte allò establert a l'article 22 d'aquesta Directiva.

Una tercera possibilitat podria ser que ens trobéssim davant d'un model organitzatiu descentralitzat. En aquest cas, cada corporació local seria responsable del tractament de la informació generada per les seves actuacions i que gestiona a través del programa informàtic DRAG, i el sistema d'informació proposat només seria un mecanisme o mitjà per facilitar la tramesa de la informació que en un determinat moment pugui requerir un cos de policial local a un altre cos de policia local per a l'exercici de llurs funcions.

En qualsevol cas, la definició de quin és el paper de les diferents administracions intervinents, decisió que han de prendre les entitats implicades, esdevé un element essencial per determinar les obligacions i les responsabilitats que poden correspondre a cadascuna de les administracions implicades.

V

Dit això, tant la creació d'aquest sistema d'informació policial com els fluxos informatius que es produeixin a partir de la seva posada en funcionament s'han de situar en el marc normatiu

aplicable a l'actuació de la policia local, per tal de considerar-los legítims des del punt de vista de la protecció de dades personals.

D'acord amb l'LOPD, la creació de fitxers policials, així com el tractament i la comunicació de les seves dades, es troba restringida a les administracions públiques que tenen atribuïdes competències en matèria de seguretat pública (articles 22), entre les quals, les corporacions locals.

En aquest sentit, la Llei orgànica 2/1986, de 13 de març, reguladora de les Forces i Cossos de Seguretat de l'Estat (LOFCSE), disposa que:

> *"Artículo primero.*
> *1. La Seguridad Pública es competencia exclusiva del Estado. Su mantenimiento corresponde al Gobierno de la Nación.*
> *2. Las Comunidades Autónomas participarán en el mantenimiento de la Seguridad Pública en los términos que establezcan los respectivos Estatutos y en el marco de esta Ley.*
> *3. Las* ***Corporaciones Locales participarán en el mantenimiento de la seguridad pública en los términos establecidos en la Ley Reguladora de las Bases de Régimen Local y en el marco de esta Ley.***
> *4. El mantenimiento de la Seguridad Pública* ***se ejercerá por las distintas Administraciones Públicas a través de las Fuerzas y Cuerpos de Seguridad****."*

L'LOFCSE regula en termes generals les policies locals (Títol V) i les considera com un cos de seguretat més al costat de la policia estatal i autonòmica (article 2). Així mateix, concreta unes funcions comunes per a totes les Forces i Cossos de Seguretat (article 11).

La Llei 16/1991, de 10 de juliol, de les policies locals (LPL) incorpora aquest conjunt de funcions en el seu text legal.

Així, d'acord amb l'article 11 de l'LPL, correspon a les policies locals que depenen dels municipis de Catalunya, en llur àmbit d'actuació, les funcions següents:

> *"a) Protegir les autoritats de les corporacions locals i vigilar i custodiar els edificis, les instal·lacions i les dependències d'aquestes corporacions.*
> *b) Ordenar, senyalitzar i dirigir el trànsit en el nucli urbà, d'acord amb el que estableixen les normes de circulació.*
> *c) Instruir atestats per accidents de circulació esdevinguts dins el nucli urbà, en el qual cas han de comunicar les actuacions dutes a terme a les forces o els cossos de seguretat competents.*
> *d) Exercir de policia administrativa, a fi d'assegurar el compliment dels reglaments, de les ordenances, dels bans, de les resolucions i de les altres disposicions i actes municipals, d'acord amb la normativa vigent.*
> *e) Exercir de policia judicial, d'acord amb l'article 12 i amb la normativa vigent.*
> *f) Dur a terme diligències de prevenció i actuacions destinades a evitar la comissió d'actes delictuosos, en el qual cas han de comunicar les actuacions dutes a terme a les forces o els cossos de seguretat competents.*
> *g) Col·laborar amb les forces o els cossos de seguretat de l'Estat i amb la Policia Autonòmica en la protecció de les manifestacions i en el manteniment de l'ordre en grans concentracions humanes quan siguin requerides a fer-ho.*
> *h) Cooperar en la resolució dels conflictes privats, quan siguin requerides a fer-ho.*
> *i) Vigilar els espais públics.*
> *j) Prestar auxili en accidents, catàstrofes i calamitats públiques, participant, d'acord amb el que disposen les lleis, en l'execució dels plans de protecció civil.*

k) Vetllar pel compliment de la normativa vigent en matèria de medi ambient i de protecció de l'entorn.
l) Dur a terme les actuacions destinades a garantir la seguretat viària en el municipi.
m) Qualsevol altra funció de policia i de seguretat que, d'acord amb la legislació vigent, els sigui encomanada."

Per tant, les policies locals dels ajuntaments (amb la denominació de policia local, policia municipal, guàrdia urbana o altres de tradicionals) resten legitimades per dur a terme els tractaments de dades personals que requereixin per a l'exercici de les funcions legalment encomanades.

Pel que fa concretament a la possibilitat de compartir aquest tipus d'informació, cal tenir present que la legislació aplicable preveu una obligació de col·laboració entre les Forces i Cossos de Seguretat de l'Estat per a l'exercici i desenvolupament del conjunt de funcions que tenen atribuïdes, que abasta també el deure de comunicar aquella informació que pugui resultar rellevant i necessària a tal efecte.

Sobre aquesta qüestió, l'LOFCSE disposa que *"los miembros de las Fuerzas y Cuerpos de Seguridad* ***ajustarán su actuación al principio de cooperación recíproca*** *y su coordinación se efectuará a través de los órganos que a tal efecto establece esta Ley*" (article 3).

També que *"los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos de Policía de las Comunidades Autónomas* ***deberán prestarse mutuo auxilio e información recíproca*** *en el ejercicio de sus funciones respectivas"* (article 45 LOFCSE).

D'acord amb la Llei 4/2003, de 7 d'abril, d'ordenació del sistema de seguretat pública de Catalunya, la policia de la Generalitat-mossos d'esquadra i les policies dels ajuntaments constitueixen la policia de les institucions pròpies de Catalunya (article 5).

Aquesta mateixa Llei 4/2003 regula els principis als quals han d'atenir-se les administracions públiques amb competències sobre seguretat, entre els quals destaca el d'*"****informació recíproca****, especialment quan calgui per complir millor les competències de cada administració"* (article 21.b)).

En aquest sentit, la Llei disposa que *"les autoritats i els membres del cos de la policia de la Generalitat-mossos d'esquadra i dels cossos de policia local de Catalunya estan obligats a facilitar-se mútuament la informació que sigui rellevant per al compliment de les funcions respectives, sens perjudici de la reserva que escaigui per raó de la matèria i amb ple respecte de la legislació aplicable, en particular la relativa a la protecció de dades personals"* (article 23.1 Llei 4/2003).

També cal tenir present que la mateixa LOPD legitima les comunicacions de dades personals que tinguin lloc entre administracions públiques quan aquestes tenen per finalitat l'exercici de competències idèntiques o que versin sobre una mateixa matèria.

En concret, l'article 21.1 de l'LOPD estableix que *"les dades de caràcter personal recollides o elaborades per les administracions públiques per a l'exercici de les seves atribucions no han de ser comunicades a altres administracions públiques per a l'exercici de competències diferents o de competències quan tractin matèries diferents, excepte quan la comunicació tingui com a objecte el tractament posterior de les dades amb finalitats històriques, estadístiques o científiques*". L'apartat 4 del mateix article estableix que *"en aquests casos no és necessari el consentiment de l'afectat".*

En aquest sentit, l'article 10.4.c) de l'RLOPD complementa la regulació legal assenyalant que no serà necessari el consentiment de l'interessat quan la cessió entre administracions

públiques es realitzi *"per a l'exercici de competències idèntiques o que versin sobre les mateixes matèries".*

Apuntar que, a efectes de facilitar l'intercanvi d'informació entre cossos policials, la Llei 4/2003 preveu que el departament titular de les competències en matèria de seguretat pública ha de gestionar i mantenir un sistema unificat d'informacions policials, al qual tenen accés el cos dels Mossos d'Esquadra i les policies locals de Catalunya, preveient la mateixa Llei que mitjançant conveni d'adhesió bilateral es regulin les condicions de l'accés i la participació de cada cos de policia local (article 24.2).

També que el cos de Mossos d'Esquadra ha de facilitar l'accés de les policies locals a altres bases de dades, en els supòsits d'interès local que es determinin per reglament (article 24.3 Llei 4/2003).

I, pel que fa al programa informàtic d'aplicació del cos de Mossos d'Esquadra, que mitjançant conveni s'ha preveure que les policies locals puguin usar-lo, així com el treball en xarxes integrades d'informació policial (article 24.4 Llei 4/2003).

En la consulta s'apunta que el sistema d'informació que es pretén crear *"no interfereix en el tractament de la informació entre policies per mitjà del SIP o d'altres sistemes d'informació compartits"*, això és el sistema unificat d'informació policial a què fan referència les previsions esmentades de la Llei 4/2003.

Es tracta, se sosté en la consulta, d'un sistema *"complementari i en cap cas es deixarà de carregar o compartir la informació necessària o obligatòria al SIP per poder dur a terme les funcions i tasques policials regulades per les lleis."*

Fer notar, en aquest punt, que la Llei 4/2003 disposa que *"el Govern, per mitjà del departament titular de les competències en matèria de seguretat pública, té la responsabilitat de fer efectiva la coordinació de les policies locals, la qual implica la determinació dels mitjans i dels sistemes de relació que fan possible l'acció conjunta d'aquests cossos, mitjançant les autoritats competents, de manera que s'aconsegueixi la integració de les actuacions particulars respectives dins el conjunt del sistema de seguretat que els és confiat"* (article 25.1).

També l'LPL disposa que *"als efectes d'aquesta Llei, s'entén per "coordinació" la determinació dels mitjans i dels sistemes de relació que fan possible l'acció conjunta de les policies locals, mitjançant les autoritats competents, de manera que s'aconsegueixi la integració de les actuacions particulars respectives dins el conjunt del sistema de seguretat ciutadana que els és confiat"* (article 14).

Sobre aquesta qüestió, l'article 15 de l'LPL concreta que:

> *"1. La coordinació de l'activitat de les policies locals es pot estendre, en tot cas, a les funcions següents:*
> *a) Promoure l'homogeneïtzació dels mitjans tècnics i la uniformitat dels altres elements comuns.*
> *b) Establir els instruments i els mitjans que facin possible un sistema d'informació recíproca.*
> *(...)."*

Vist això, si bé podria dir-se que, des de la vessant de la protecció de dades, existiria suficient cobertura legal per a l'intercanvi, entre cossos de policia local, d'aquella informació personal que pugui ser d'interès per a l'exercici de les funcions que legalment tenen atribuïdes, la creació d'un sistema d'informació com el que es proposa a la consulta sembla que requeriria de la

intervenció del departament competent en matèria de seguretat pública de l'Administració de la Generalitat.

En qualsevol cas, fer notar que, des del punt de vista de la protecció de dades personals, és necessari vetllar perquè qualsevol d'aquestes comunicacions d'informació policial, a banda de comptar amb legitimació suficient, s'adeqüin, entre d'altres, al principi de qualitat de les dades (article 4 LOPD).

Aquest principi, en la seva vessant de limitació de la finalitat i minimització de dades, exigeix que les dades personals han d'ésser recollides amb fins determinats, explícits i legítims, no sent possible el seu tractament posterior de manera incompatible amb aquests fins, i han d'ésser adequades, pertinents i limitades al que és necessari per assolir aquests fins que justifiquen el seu tractament.

Cal tenir en consideració, per tant, que els accessos o comunicacions de dades que tinguin lloc arran la posada en funcionament del present sistema d'informació només podran considerar-se adequats a la normativa de protecció de dades en la mesura que es limitin a les dades personals que cada cos de la policia local requereixi per a l'exercici de les funcions que, de conformitat amb la legislació aplicable, siguin de la seva competència, i sempre que aquestes dades siguin necessàries, pertinents i adequades en cada cas.

Aquest mateix principi, en la seva vessant d'exactitud de les dades, també exigeix que les dades personals siguin exactes i posades al dia de manera que responguin amb veracitat a la situació actual de l'afectat. Per aquest motiu, és també necessari preveure mecanismes que garanteixin la qualitat de la informació personal incorporada en el sistema d'informació policial, de tal manera que les dades que es tractin siguin exactes i actualitzades en tot moment, qüestió que es podria veure dificultada si es produís la coexistència de sistemes d'informació paral·lels amb objectius coincidents, encara que sigui només parcialment.

VI

Per altra banda, pel que fa a la implementació del sistema d'informació, fer avinent la necessitat d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries que garanteixin la seguretat de les dades i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposades, tant si provenen de l'acció humana o del medi físic o natural (article 9 LOPD).

Sobre aquesta qüestió, recordar que el nou marc europeu regulador del dret a la protecció de dades personals (tant la Directiva 2016/680 com l'RGPD) configura un sistema de seguretat que es basa en determinar, arran d'una prèvia valoració dels riscos, quines mesures tècniques i organitzatives cal aplicar per garantir els nivells de seguretat adequats al risc en cada cas.

Aquest nou model es fonamenta en el principi de responsabilitat proactiva de manera que no només s'ha de complir la norma, sinó que també s'ha de poder demostra-ho, i en la protecció de les dades des del disseny i per defecte, de tal manera que tant en el moment de definir les diferents operacions de tractament, com a l'hora de determinar i aplicar els mitjans que s'utilitzaran per tractar les dades personals, es tindran en compte els principis, els drets i les obligacions que recull la normativa de protecció de dades personals que sigui d'aplicació als tractaments que es pretenen dur a terme.

Per tant, és necessari fer aquesta anàlisi de riscos amb caràcter previ a la posada en funcionament del sistema d'informació per determinar les mesures de seguretat tècniques i organitzatives apropiades per salvaguardar el dret a la protecció de dades dels possibles

afectats.

Apuntar, en relació amb la determinació d'aquestes mesures, que l'esquema de mesures de seguretat previst al RLOPD, si bé a hores d'ara seria d'obligat compliment, podria no ser suficient un cop es transposi la Directiva 2016/680. En alguns supòsits aquest esquema es podrà seguir aplicant, si de l'anàlisi de riscos previ es conclou que les mesures són realment les més adequades per oferir un nivell de seguretat adequat al cas concret, però en d'altres pot ser necessari completar-les amb mesures addicionals fruit de l'anàlisi de riscos.

En la consulta es fa referència expressa a la implementació d'un registre d'accessos, de tal manera que, per a cada accés, es preveu enregistrar el nom de l'usuari del sistema, el dia i hora de l'accés, les dades consultades i el motiu de la consulta.

Més enllà de valorar positivament la implementació d'aquesta mesura de seguretat, fer avinent la necessitat d'avaluar l'adopció d'altres mesures addicionals, com per exemple l'establiment de mecanismes apropiats que permetin la correcta identificació i autenticació dels usuaris del sistema d'informació als efectes de garantir que no es produiran tractaments no autoritzats, entre d'altres.

Cal tenir present, vist l'article 29.2 de la Directiva 2016/680 (a l'espera de la norma de transposició), que les mesures de seguretat a implementar en un cas com el que s'examina haurien d'anar adreçades en tot cas a:

> *"a) denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento (control de acceso a los equipamientos);*
> *b) impedir que los soportes de datos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas (control de los soportes de datos);*
> *c) impedir que se introduzcan sin autorización datos personales conservados, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización (control del almacenamiento);*
> *d) impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos (control de los usuarios);*
> *e) garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado solo puedan tener acceso a los datos personales para los que han sido autorizados (control del acceso a los datos);*
> *f) garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse o a cuya disposición pueden ponerse los datos personales mediante equipamientos de comunicación de datos (control de la transmisión);*
> *g) garantizar que pueda verificarse y constatarse a posteriori qué datos personales se han introducido en los sistemas de tratamiento automatizado y en qué momento y por qué persona han sido introducidos (control de la introducción);*
> *h) impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte);*
> *i) garantizar que los sistemas instalados puedan restablecerse en caso de interrupción (restablecimiento);*
> *j) garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados (fiabilidad) y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema (integridad)."*

També, cal dir, seria necessària l'adopció i la implantació de mesures de formació del personal que ha de tractar les dades personals en qüestió.

En tot cas, fer avinent que aquestes mesures de seguretat haurien d'ajustar-se a l'Esquema Nacional de Seguretat (article 1 Reial Decret 3/2010, de 8 de gener).

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

Conclusions

És necessari definir les responsabilitats dels diferents agents implicats en la implementació d'aquest sistema d'informació per determinar les obligacions i les responsabilitats de cadascun d'ells.

Existeix habilitació per a l'intercanvi d'informació entre els diferents cossos policials, sempre d'acord amb la coordinació feta pel Departament competent en matèria de policies locals, però cal respectar el principi de qualitat de les dades, el principi d'exactitud i, prèvia anàlisi de riscos, determinar les mesures de seguretat adequades per garantir els drets de les persones afectades.

Barcelona, 30 de novembre de 2020