L'ÚS I LA PROTECCIÓ DE LES DADES PERSONALS

ESTHER MITJANS PERELLÓ
Directora de l'Agència Catalana de Protecció de Dades

1. LA NORMATIVA: GARANTIES I LÍMITS

El dret a la protecció de dades personals és transversal, és a dir, està implicat en totes les activitats que porten a terme les administracions públiques, en el sentit més ampli del terme. En l'àmbit de la investigació penal, podríem dir que hi és present de manera encara més intensa, perquè tota investigació es basa en la recopilació d'informació i, en aquest cas, en recopilació d'informació relativa a persones.

La normativa de protecció de dades estableix una sèrie de garanties per al dret a la protecció de dades, que busquen, en últim terme, que la persona pugui controlar allò que els altres —entitats públiques i privades— fan amb la informació que fa referència a la seva vida; en definitiva, estableix obligacions per als qui tracten dades personals. En el cas de les administracions públiques, la normativa de protecció de dades estableix obligacions, però també un gran nombre de prerrogatives, per tal que puguin desenvolupar les seves funcions.

El dret a la protecció de dades és autònom i és també un instrument de garantia de la resta de drets i llibertats fonamentals. Moltes vegades es vincula a la intimitat, l'honor i la pròpia imatge, però hem de recordar que amb el tractament de dades es poden vulnerar tot un conjunt de drets: llibertat sindical, llibertat de circulació, presumpció d'innocència...

Una part important dels límits al dret a la protecció de dades es basa, justament, en la defensa de l'Estat, la seguretat pública, la protecció dels drets i les llibertats de tercers, les necessitats de les investigacions que es porten a terme o la persecució d'infraccions penals.

En concret, a la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades personals (LOPD), trobem una regulació específica sobre el tractament de dades per a les forces i els cossos de seguretat.

Però, abans d'entrar en aquesta regulació específica, crec important identificar dues qüestions: d'una banda, què és una dada de caràcter personal; d'altra banda, què és un fitxer i un tractament de dades personals.

Quant a la primera qüestió, tot i que en un primer moment pugui semblar una obvietat, crec que no ho és tant. Segurament, tothom té present quina és la definició de dada personal de la LOPD:

> ...qualsevol informació referent a persones físiques identificades o identificables.

No cal insistir, doncs, en el fet que la normativa de protecció de dades només protegeix les persones físiques.

Però potser sí que és important aturar-se un moment en què vol dir *identificables* i incorporar la definició que ens ha donat, en el seu article 5.1.*o)*, el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (RLOPD):

> Persona 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 la dita identificació requereix terminis o activitats desproporcionats.

Caldria delimitar, per tant, què vol dir *terminis o activitats desproporcionats*. I, en el cas de les forces i els cossos de seguretat, la delimitació d'aquest concepte potser ha de generar una atenció especial, ateses les possibilitats de recopilació d'informació de què disposen, no solament d'àmbit nacional sinó també internacional.

La segona qüestió en què vull parar esment és la definició de *fitxer* i de *tractament de dades* de la LOPD:

> Fitxer: qualsevol conjunt organitzat de dades de caràcter personal, sigui quina sigui la forma o la modalitat de creació, emmagatzematge, organització i accés.
>
> 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.

Però, a banda de la conceptualització, vull recordar que quan parlem de *fitxers* parlem tant de fitxers manuals com de fitxers automatitzats. I que, quan ens referim a *tractament*, parlem de qualsevol acció que fem amb dades personals, encara que només sigui recollir-les.

2. LA NORMATIVA DE PROTECCIÓ EN EL TRACTAMENT DE DADES A LES FORCES I ELS COSSOS DE SEGURETAT

Fetes les apreciacions anteriors, em centraré en les particularitats que podem trobar a la normativa de protecció de dades respecte del tractament de dades per part de les forces i els cossos de seguretat.

Ja en el moment de definir l'àmbit d'aplicació de la LOPD, s'estableix que els tractaments de dades procedents d'imatges i sons obtinguts per les forces i els cossos de seguretat mitjançant la utilització de videocàmeres es regeixen per les seves disposicions específiques, i per allò que prevegi específicament la LOPD. Per ajudar a la integració de les diferents normes jurídiques, l'Agència va publicar, l'any 2009, una Instrucció en aquesta matèria amb la qual es pretén afavorir el compliment de les obligacions establertes a la normativa de protecció de dades. Aquesta Instrucció pot ser útil en tot allò que no estigui regulat per la norma especial.

Pel que fa al principi vertebrador del dret a la protecció de dades —el consentiment—, també trobem una sèrie d'excepcions en relació amb la necessitat o no d'obtenir-lo, quan les dades les recullen les administracions públiques en general i, particularment, les forces de seguretat.

Concretament, l'article 6 de la LOPD estableix que les administracions no han d'obtenir el consentiment de les persones titulars de les dades, per al seu tractament, quan siguin necessàries per a l'exercici de les seves funcions en l'àmbit de les seves competències, ni quan es refereixin a les parts d'una relació administrativa i siguin necessàries per mantenir-la o complir-la.

Convé afegir que tampoc no caldria el consentiment quan el tractament de les dades tingui com a finalitat protegir un interès vital de la persona interessada.

D'altra banda, a l'article 22 de la LOPD trobem la regulació específica aplicable al tractament de dades per part de les forces de seguretat. En aquest cas, la normativa de protecció de dades diferencia dos supòsits de tractament:

a) En primer lloc, els fitxers que continguin dades personals recollides per a finalitats administratives. Aquests fitxers estan subjectes al règim general de la normativa de protecció de dades.

b) En segon lloc, la recollida i el tractament de dades personals per a finalitats policials. És en aquest segon supòsit que la LOPD estableix una sèrie de requisits per al tractament de les dades sense consentiment del seu titular, diferenciant el tractament de les dades especialment protegides (ideologia, religió, creences, afiliació sindical, salut, origen racial i vida sexual).

Quan el tractament de les dades personals no es refereix a les especialment protegides, es permet la recollida i el tractament de les que siguin estrictament necessàries per a la prevenció d'un perill real per a la seguretat pública o per a la repressió d'infraccions penals. En aquest casos, les dades s'han d'emmagatzemar en fitxers específics establerts a aquest efecte i s'han de classificar per categories en funció del grau de fiabilitat.

Podem observar que apareixen conceptes jurídics indeterminats que donen un cert marge d'interpretació: «estrictament necessàries», «perill real»...

Però també es preveu específicament l'excepció al consentiment, quan es tracta de la recollida i el tractament de dades especialment protegides o sensibles. En aquest cas, es poden tractar en els supòsits en què sigui absolutament necessari per a les finalitats d'una investigació concreta. Veiem que, també aquí, es tornen a utilitzar conceptes indeterminats com «absolutament necessari».

3. PRINCIPIS DE QUALITAT DE LES DADES

Vist l'ampli marge d'interpretació, crec que és important aplicar de manera rigorosa altres principis establerts a la normativa de protecció de dades. Parlo dels principis de qualitat de les dades, que es poden resumir en:

— principi de finalitat
— principi de proporcionalitat
— principi de conservació
— principi de lleialtat

Bàsicament, es tractaria de ser conscients que les dades només poden ser recollides i tractades quan siguin adequades, pertinents i no excessives, en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut. Per tant, cal identificar amb claredat les finalitats per a les quals es recullen les dades i no utilitzar-les per a finalitats diferents.

Com que aquest principi pot ser matisat en l'àmbit de la investigació de delictes, cal centrar l'atenció en el principi de proporcionalitat, en el sentit de parar-nos a pensar quines són les dades que, efectivament, són necessàries per a la investigació que portem a terme o per a la prevenció del perill que volem evitar. En definitiva, es pot dir que cal utilitzar sempre el mecanisme que sigui menys intrusiu en els drets de les persones.

No podem oblidar que en els darrers temps s'ha tendit a la recopilació massiva d'informació sense establir, probablement, uns criteris per mirar de definir la informació rellevant per al cas concret en què s'està treballant.

Un altre dels principis de protecció de dades es refereix a la seva exactitud; principi que, també en l'àmbit que avui tractem, de vegades es dilueix una mica, però que la mateixa LOPD ja ha previst, en referir-se als terminis de conservació de la informació i a la manera de conservar-la. Així, hem de tenir present que les dades personals registrades amb finalitats policials s'han de cancel·lar quan no siguin necessàries per a les investigacions que n'hagin motivat la recollida. Per tal de delimitar aquesta qüestió, s'ha de valorar especialment:

— l'edat de la persona afectada i el caràcter de les dades emmagatzemades,
— la necessitat de mantenir les dades fins a concloure una investigació o un procediment concret,
— la resolució judicial ferma, especialment l'absolutòria, l'indult, la rehabilitació i la prescripció de responsabilitat.

És important tenir present que cancel·lar no vol dir necessàriament suprimir la informació, sinó que el RLOPD ens indica que la cancel·lació és el procediment en virtut del qual el responsable cessa en l'ús de les dades. Així, la cancel·lació implica el bloqueig: identificar i reservar les dades, amb la finalitat d'impedir-ne el tractament, excepte per posar-les a disposició de les administracions públiques, jutges i tribunals, per a l'atenció de les possibles responsabilitats nascu-

3. PRINCIPIS DE QUALITAT DE LES DADES

Vist l'ampli marge d'interpretació, crec que és important aplicar de manera rigorosa altres principis establerts a la normativa de protecció de dades. Parlo dels principis de qualitat de les dades, que es poden resumir en:

— principi de finalitat
— principi de proporcionalitat
— principi de conservació
— principi de lleialtat

Bàsicament, es tractaria de ser conscients que les dades només poden ser recollides i tractades quan siguin adequades, pertinents i no excessives, en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut. Per tant, cal identificar amb claredat les finalitats per a les quals es recullen les dades i no utilitzar-les per a finalitats diferents.

Com que aquest principi pot ser matisat en l'àmbit de la investigació de delictes, cal centrar l'atenció en el principi de proporcionalitat, en el sentit de parar-nos a pensar quines són les dades que, efectivament, són necessàries per a la investigació que portem a terme o per a la prevenció del perill que volem evitar. En definitiva, es pot dir que cal utilitzar sempre el mecanisme que sigui menys intrusiu en els drets de les persones.

No podem oblidar que en els darrers temps s'ha tendit a la recopilació massiva d'informació sense establir, probablement, uns criteris per mirar de definir la informació rellevant per al cas concret en què s'està treballant.

Un altre dels principis de protecció de dades es refereix a la seva exactitud; principi que, també en l'àmbit que avui tractem, de vegades es dilueix una mica, però que la mateixa LOPD ja ha previst, en referir-se als terminis de conservació de la informació i a la manera de conservar-la. Així, hem de tenir present que les dades personals registrades amb finalitats policials s'han de cancel·lar quan no siguin necessàries per a les investigacions que n'hagin motivat la recollida. Per tal de delimitar aquesta qüestió, s'ha de valorar especialment:

— l'edat de la persona afectada i el caràcter de les dades emmagatzemades,
— la necessitat de mantenir les dades fins a concloure una investigació o un procediment concret,
— la resolució judicial ferma, especialment l'absolutòria, l'indult, la rehabilitació i la prescripció de responsabilitat.

És important tenir present que cancel·lar no vol dir necessàriament suprimir la informació, sinó que el RLOPD ens indica que la cancel·lació és el procediment en virtut del qual el responsable cessa en l'ús de les dades. Així, la cancel·lació implica el bloqueig: identificar i reservar les dades, amb la finalitat d'impedir-ne el tractament, excepte per posar-les a disposició de les administracions públiques, jutges i tribunals, per a l'atenció de les possibles responsabilitats nascu-

des del tractament i només durant el termini de prescripció de les responsabilitats esmentades.

Un altre dels principis que defineixen el dret a la protecció de dades és el dret d'informació en el moment de la recollida de les dades. Aquest dret comporta l'obligació d'aquells que tracten les dades personals d'informar la persona titular de quines seran les circumstàncies del tractament (responsable del fitxer, fitxer on s'incorporaran les dades, finalitats i usos, obligació o no de facilitar les dades i lloc on exercir els drets d'accés, rectificació i cancel·lació, entre d'altres qüestions). En definitiva, informació que permeti a la persona titular de les dades conèixer què se'n farà.

En el cas del dret d'informació hi ha poques excepcions, fins i tot per a les administracions públiques. Tot i aquesta afirmació, la LOPD també ha introduït alguna particularitat en aquest sector, indicant que el dret d'informació en el moment de la recollida de les dades no és aplicable quan el fet d'informar-ne la persona interessada afecti la defensa nacional, la seguretat pública o la persecució d'infraccions penals.

Un altre dels àmbits on també s'introdueixen excepcions és l'exercici dels drets d'accés, rectificació i cancel·lació. La LOPD estableix que els responsables de fitxers amb finalitats policials poden denegar l'accés, la rectificació o la cancel·lació en funció dels perills que en puguin derivar per a la defensa de l'Estat o la seguretat pública, la protecció dels drets i les llibertats de tercers o les necessitats de les investigacions que s'estiguin duent a terme.

4. LES CESSIONS DE DADES

Un dels camps on sorgeixen més problemàtiques és el de les cessions de dades. Hem vist que, quan es tracta de recollir i tractar dades amb finalitats policials, no cal el consentiment de la persona interessada; per tant, és particularment important que la resta de principis s'apliquin de manera rigorosa. És necessari doncs, que les forces i els cossos de seguretat formulin la petició d'informació personal d'acord amb el que disposen les lleis aplicables, atès que es tracta de supòsits d'excepció on decau el consentiment previ del titular per atendre altres interessos públics; és el cas, per exemple, de la protecció de la seguretat ciutadana.

Així, l'Agència, en la resolució d'una consulta que se li va formular, ja va indicar que, en termes generals, l'Administració pública o el personal funcionari al qual es requereixin determinades dades de caràcter personal pot sol·licitar, a l'efecte de poder justificar la comunicació de les dades, un aclariment del motiu que fonamenta la petició de les forces i els cossos de seguretat. Això, si aparentment no es tracta de cap dels supòsits habilitats o si no es dedueix clarament que són unes dades necessàries per a la prevenció d'un perill real per a la seguretat pública, o per a la repressió d'infraccions penals, sens perjudici que correspongui a les forces i els cossos de seguretat l'apreciació dels fets o de les circumstàncies de la seva actuació.

Així mateix, vull recordar que la normativa de protecció de dades estableix altres supòsits que legitimen la cessió de dades sense el consentiment previ dels

seus titulars. D'una banda, trobem l'article 11.2 de la LOPD, on s'estableixen una sèrie d'excepcions, de les quals crec important mencionar-ne dues:

a) quan la cessió està autoritzada en una llei;
b) quan la comunicació que s'hagi d'efectuar tingui com a destinatari el Síndic de Greuges, el Ministeri Fiscal, els jutges o tribunals o la Sindicatura de Comptes, en l'exercici de les funcions que tenen atribuïdes.

I, respecte de les cessions de dades entre administracions públiques, l'article 21 de la LOPD estableix aquesta possibilitat, sense el consentiment del titular, quan es comuniquin per a l'exercici de les mateixes competències o de competències que tractin les mateixes matèries.

5. EL PRINCIPI DE SEGURETAT

Finalment, quant a les obligacions derivades de la normativa de protecció de dades, cal recordar que els fitxers o tractament de dades han de complir el principi de seguretat, és a dir, establir les mesures que n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat. En el títol VIII del RLOPD, trobem l'estàndard mínim de seguretat a aplicar sobre els fitxers automatitzats i sobre els fitxers manuals. Concretament, en la definició dels nivells de seguretat aplicables, el Reglament estableix que correspon el nivell alt de seguretat als fitxers o tractaments de dades que:

a) es refereixin a dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual;
b) els que continguin dades derivades d'actes de violència de gènere;
c) i tots els que continguin o es refereixin a dades obtingudes per a fins policials.

Per tant, el nivell de seguretat a aplicar, per defecte, ha de ser el més elevat que es regula en el RLOPD.

En l'àmbit de la seguretat pública, el dret a la protecció de dades personals està notablement limitat i entra en conflicte constant amb els interessos que es persegueixen en matèria de seguretat. Justament en aquest marc, com hem vist, dos dels eixos principals del dret a la protecció de dades estan força restringits: el dret a la informació en el moment de la recollida de les dades i el consentiment per al seu tractament.

6. CONCLUSIÓ

L'Agència Catalana de Protecció de Dades ja fa uns anys que està treballant en el que anomenen el model català de protecció de dades, que ha permès definir una sèrie de mesures que tendeixen a la prevenció. Partint de la idea que el dret a la protecció de dades és de difícil reparació un cop vulnerat, del que es tractaria és d'es-

tablir mecanismes tècnics, organitzatius i de procediment que garanteixin el compliment dels principis reguladors del dret a la protecció de dades i, alhora, millorin la gestió de la informació i, per tant, de les actuacions que es porten a terme.

El dret a la protecció de dades no és només un conjunt d'obligacions per a les entitats, sinó que també pot ser un important instrument per generar la confiança de la ciutadania. Això pot reforçar el principi establert a l'article 104 de la Constitució, segons el qual les forces i els cossos de seguretat tenen com a missió protegir el lliure exercici dels drets i llibertats, a més de garantir la seguretat ciutadana.

Aquesta confiança només es pot crear si dissenyem entorns col·laboratius que tinguin en compte la privacitat i la protecció de dades personals, tenint en compte l'especial rellevància que pren la seguretat de la informació en l'entorn analitzat, atès que altres principis queden molt limitats. També és important un canvi de, diguem-ne, «consciència» respecte del tractament de les dades personals, que passa per la formació i la informació de tothom qui hagi de gestionar dades personals en el desenvolupament de les seves funcions.

En definitiva, és qüestió de gestionar correctament la informació que estem legitimats a tractar, sense oblidar que cap dret és absolut però que tampoc es pot veure tan limitat que deixi de tenir virtualitat. Com en molts altres àmbits, haurem de fer un esforç de ponderació.