Noves tecnologies, videovigilància, dret a la protecció de dades i fitxers policials[1]

IGNACIO VILLAVERDE MENÉNDEZ

Professor titular de dret constitucional i
secretari general de la Universitat d'Oviedo

1. UNES CONSIDERACIONS GENERALS

Convé que iniciem aquestes reflexions tot recordant que la protecció de dades no es redueix exclusivament a l'àmbit d'aplicació de la Llei orgànica 15/1999, de 13 de desembre, de protecció de les dades de caràcter personal (en endavant, LOPD). El Tribunal Constitucional (en endavant, TC) ha declarat, en la Sentència 292/2000, que la protecció de les dades personals és un dret fonamental que deriva de l'article 18.4 de la Constitució espanyola de 1978 (en endavant, CE). Com a tal, si se'm permet l'expressió, té una vida pròpia al marge de la LOPD, i aquesta es limita a desenvolupar el dret, i a regular-ne l'exercici en algun dels seus extrems, en aquells àmbits que resulten d'allò que s'ha disposat en els seus articles 2 i 3; però que no esgota l'àmbit d'aplicació del dret fonamental a la protecció de les dades personals. Cal advertir, a més a més, que l'aplicació de la LOPD està condicionada al fet que les dades personals siguin objecte de registre «en suport físic, que les faci susceptibles de tractament, i a tota modalitat d'ús posterior d'aquestes dades pels sectors públic i privat» (art. 2.1 LOPD); es considera «tractament» les «operacions i procediments tècnics de caràcter automatitzat o no, que permetin la recollida, enregistrament, conservació, elaboració, modificació, bloqueig i cancel·lació, així com les cessions de dades que resultin de comunicacions, consultes, interconnexions i transferències» (art. 3.c) LOPD). La forma més gràfica d'explicar això és que, després de les SSTC 290 i la STC 292/2000, seria indiferent que existís o no la LOPD o una norma reguladora de la protecció de dades. La raó

1. Aquest text és la transcripció revisada de la intervenció del seu autor en el Curs les ponències del qual constitueixen el contingut d'aquest llibre. Aprofito aquestes línies per agrair al professor Vicenç Aguado, i a l'Escola de Policia de Catalunya, en la persona del seu director, el senyor Joan Mauri i Majós, la seva amable i generosa invitació perquè participés en aquest prestigiós Curs sobre Seguretat Pública i Privada.

d'això és que la protecció de dades ja és un dret fonamental dotat d'eficàcia directa amb un contingut constitucional definit en aquestes sentències i que, a més a més, és d'aplicació general (àmbit objectiu) i universal (àmbit subjectiu). Quant al dret fonamental, per tant, no hi ha excepcions d'aplicació, però sí que n'hi ha, en canvi, en l'aplicació de la LOPD. És important no perdre de vista aquesta proposició per entendre exactament algunes de les qüestions que s'abordaran en les pàgines vinents.

Un altre apunt de la importància que tindrà en aquestes pàgines és el referit als fins constitucionalment legítims de l'actuació de les Forces i Cossos de Seguretat de l'Estat, de les comunitats autònomes on n'hi hagi i dels ens locals (en endavant, FFCCSS). Aquest apunt està lligat, evidentment, als dos últims punts d'aquest opuscle on es descriu la interactuació de la protecció de dades i la intercepció de les telecomunicacions i la videovigilància. L'enfocament d'aquestes pàgines serà sempre el de la perspectiva de les obligacions que a les FFCCSS imposa la garantia del dret fonamental a la protecció de les dades personals i les que resulten del desenvolupament d'aquest dret fonamental per la LOPD.

Les tesis que es tractarà de sostenir aquí són, en primer lloc, que el canvi d'objecte o de mitjà o de tècnica, el fet que ja no es parli de correu postal o de «telèfon» sinó de correu electrònic o de «mòbils» d'última generació o de mitjans telemàtics o electrònics de comunicació, no canvia en absolut el sistema de garanties constitucionals en matèria d'intercepció de les comunicacions. El contingut del dret fonamental al secret de les comunicacions de l'article 18.3 CE continua sent el mateix sigui quin sigui el mitjà empleat per comunicar-se o per interceptar la comunicació. Per tant, l'article 579 LECrim continua aplicant-se tant si parlem d'una carta o d'un correu electrònic o d'una trucada a un telèfon fix, o bé una comunicació electrònica a través d'un SMS, etc. Els avenços de la tecnologia no suposen, al nostre parer, cap canvi en l'estructura ni en el contingut de les garanties constitucionals relatives al secret de les comunicacions o a la protecció de dades.

En segon lloc, i com ja es va dir, el règim jurídic de la protecció de dades no es limita al que disposa la LOPD. Així, per exemple, encara que la LOPD exclou del seu àmbit d'aplicació «els fitxers establerts per a la investigació del terrorisme i de formes greus de delinqüència organitzada» (art. 2.2.c), no per això les investigacions policials en matèria de terrorisme o de l'activitat delictiva organitzada són un espai immune exempt de les garanties constitucionals de la protecció de dades.

En tercer lloc, cal distingir l'activitat de prevenció unida a la garantia de la seguretat pública, d'encaixament constitucional en l'article 104 CE, de l'activitat repressiva del delicte; és a dir, entre la *policia administrativa de seguretat* on l'actuació de les FFCCSS van dirigides a un fi molt específic com és el de la prevenció del dany en béns i persones, i la *policia judicial*, que es mou en un pla diferent, que és el de la lluita processal i judicial contra la delinqüència. Són plans diferents constitucionalment, i responen a esquemes i estructures de garanties també distintes. El legislador conscientment o inconscientment ha tingut present aquesta distinció. N'és una prova el fet que quan la Llei orgànica 4/1997, de 4 d'agost, reguladora de la utilització de videocàmeres per les Forces i Cossos de Seguretat de l'Estat de Videovigilància (en endavant, LOV), normativitza la instal·lació de les videocàmeres

fixes, o fa el mateix per a l'ús de videocàmeres mòbils, ho fa a l'efecte de l'exercici de les funcions pròpies de la *policia administrativa*. En canvi, quan les FFCCSS actuen en la condició de *policia judicial*, el marc de la seva actuació en matèria de videovigilància no és la LOV, per la qual cosa n'han de remetre el règim a la LECrim i no a la LOV.

És prou clar que el context normatiu resulta bastant complex i dens. Tractarem d'agrupar-lo en tres grans sectors. Un relatiu a la *policia administrativa de seguretat*, un altre al de *policia judicial* i, finalment, un altre àmbit que sol eludir-se, però que és d'enorme importància, que és el referit a l'actuació dels serveis secrets; en el cas espanyol, del Centre Nacional d'Intel·ligència (CNI).

Qualsevol de les activitats que seran objecte d'estudi en aquest treball suposa demanar i tractar dades de caràcter personal, sigui en suport digital o bé en qualsevol altre suport emprat. Cal recordar que dada personal és qualsevol informació concernent a persones físiques identificades o identificables (art. 3.a) LOPD, i que la STC 292/2000 va elevar a definició de l'objecte del dret fonamental a la protecció de les dades personals), la qual cosa s'estén també a les imatges de les persones, sempre que en permeti la identificació.[2] No cal oblidar que el dret fonamental a la protecció de les dades personals i la pròpia LOPD s'apliquen a qualsevol mena de mitjà que suporti la dada personal (analògic o digital). Però no hi ha dubte que la intercepció de comunicacions o la enregistrament d'imatges i sons també afecta molts altres drets fonamentals (a vegades, afecten també la llibertat d'expressió i informació o al dret a l'honor).[3] Primer de tot, ens interessa, fonamentalment,

2. *Mutatis mutandis*, val la pena transcriure aquí el següent Informe de l'Agència Espanyola de Protecció de Dades sobre videovigilància al lloc de treball (2001): «Es va plantejar si resulta conforme a allò que s'ha establert en la LOPD la instal·lació de càmeres per al control de l'activitat dels treballadors de l'entitat consultant. La primera qüestió a resoldre va ser discernir si les imatges i sons que s'obtindrien per tals sistemes de registre estaven sotmesos al que disposa l'esmentada llei orgànica. Per a això va ser necessari efectuar dues acotacions prèvies: *a*) En primer lloc, es planteja el problema de si les esmentades imatges i sons poden ser considerats com a dades de caràcter personal, de conformitat amb allò que s'ha establert en la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal. A aquest efecte, i amb caràcter general, cal indicar que els articles 1 i 2 de l'esmentada llei estenen la seva protecció als drets dels ciutadans pel que fa al tractament automatitzat de les seves dades de caràcter personal, sent definides aquestes en l'article 3.a) de la Llei orgànica com "qualsevol informació concernent a persones físiques identificades o identificables". *b*) En segon lloc, i malgrat que ens trobem davant un supòsit en què hi hagi dades de caràcter personal, serà necessari que aquestes dades estiguin incorporades a un fitxer, definit com "tot conjunt organitzat de dades de caràcter personal, qualsevol que fos la forma o modalitat de la seva creació, emmagatzemament, organització i accés", per l'article 3.b) de la llei. Doncs bé, en relació amb el primer dels criteris a què s'ha fet referència, cal indicar que les imatges a què es refereix la consulta només podran ser considerades dades de caràcter personal en el cas que permetin la identificació de les persones que hi apareixen, i no estaran emparades en la llei orgànica en cas contrari. Així, en els supòsits en què les imatges es fessin del lloc de treball sí que es produiria l'esmentada identificació, atès que sempre hi apareixerien els treballadors de l'empresa al seu lloc d'activitat (cosa que els fa perfectament identificables). Pot consultar-se en www.agpd.es, en les seccions "Canal de documentació", "Informes", "Altres qüestions d'interès"».

3. El tema de les telecomunicacions s'ha posat d'especial relleu en l'actualitat diària com a resultat de l'anunci per part de les autoritats de la Unió Europea, que ha estat corejat amb una certa imprudència per part del nostre ministre de l'Interior, respecte de la intercepció, ús i tractament de les dades que ell anomena objectius de les comunicacions entre particulars. Es considera que la dada objectiva de qui està conversant, des d'on i a través de quin mitjà ho fa no afecta el secret de les comunicacions. Això és

aquests quatre drets fonamentals: protecció de dades, secret de les comunicacions, dret a la pròpia imatge i dret a la intimitat. I ens hi cenyirem.

2. El contingut constitucional de la protecció de dades

El dret fonamental a la protecció de dades personals és, indubtablement, el més nou d'allò esmentat unes línies més amunt; potser per això convindria detenir-se un instant en la definició del seu contingut.

Aquest contingut constitucional del dret fonamental a la protecció de les dades personals es concreta en una sèrie de punts molt simples però capitals. En primer lloc, la protecció de dades no és una garantia del secret de la dada sinó d'algunes condicions per a l'ús legítim per part de tercers diferents de l'afectat. Quan el TC tracta de distingir la protecció de dades del dret a la intimitat se centra en el fet que primer l'objecte de la protecció de dades no és una dada íntima sinó, precisament, un dada revelada (STC 292/2000). Allò que tracta de protegir el dret fonamental de la protecció de dades no és l'opacitat de la dada, ni la seva *intimitat* o el control sobre qui pot conèixer un dada relativa a la vida personal o familiar. Justament l'objecte de protecció del dret fonamental és la dada ja coneguda, bé perquè se n'ha consentit el coneixement per tercers, o bé perquè així ho disposa una norma. La dada ha sortit de l'esfera privada del subjecte, i ara es tracta d'establir en quines condicions el seu tráfic i la seva circulació són constitucionalment adequats.

L'objecte del dret fonamental de la protecció de dades és, per tant, el règim de coneixement, ús i destí d'un dada que ha sortit de l'àmbit de la vida privada, personal i familiar de la persona. Aquest és l'objecte del dret fonamental a les dades que dota el seu titular d'un poder jurídic de disposició sobre la publicitat de la dada personal (STC 292/2000). Aquesta és la clau de volta del règim constitucional i legal de la protecció de dades: el ple control de la persona sobre l'ús i destí de les seves dades personals. D'aquí deriven els principis de consentiment informat i finalitat que tanquen el sistema: llevat d'excepció legal, només es pot fer ús de les dades d'una persona si aquesta ha consentit i ho ha fet amb ple coneixement de les dades que seran utilitzades i amb quina finalitat, així com dels drets que l'assisteixen (accés, rectificació, cancel·lació i oposició), així mateix l'ús de les dades estarà sotmès sempre a un fi conegut per l'interessat, explícit, inequívoc, determinat i legítim.

Així ho ha expressat la STC 292/2000:

> De tot el que s'ha dit resulta que el contingut del dret fonamental a la protecció de dades consisteix en un poder de disposició i de control sobre les dades personals que faculta la persona per decidir quines d'aquestes dades proporcionarà a un ter-

---

un error atès que la jurisprudència del TEDH i del TC han afirmat de forma reiterada que el coneixement d'aquestes dades objectives també cal integrar-lo dins el camp de garanties de l'article 18.3 de la Constitució.

cer, sigui l'Estat o un particular, o quines pot aquest tercer demanar, i que també permet a l'individu saber qui posseeix aquestes dades personals i per a què, podent oposar-se a aquesta possessió o ús. Aquests poders de disposició i control sobre les dades personals, que constitueixen part del contingut del dret fonamental a la protecció de dades, es concreten jurídicament en la facultat de consentir la recollida, l'obtenció i l'accés a les dades personals, el seu posterior emmagatzemament i tractament, així com l'ús o usos possibles, per un tercer, sigui l'Estat o un particular. I aquest dret a consentir el coneixement i el tractament, informàtic o no, de les dades personals, requereix com a complements indispensables, d'una banda, la facultat de saber en tot moment qui disposa d'aquestes dades personals i a quin ús les està sotmetent, i, d'una altra, el poder oposar-se a aquesta possessió i usos.

En fi, són elements característics de la definició constitucional del dret fonamental a la protecció de dades personals els drets de l'afectat a consentir sobre la recollida i ús de les seves dades personals i a saber-ne el destí. I resulten indispensables per fer efectiu aquest contingut el reconeixement del dret a ser informat de qui posseeix les seves dades personals i amb quina finalitat, i el dret a poder oposar-se a aquesta possessió i ús requerint a qui correspongui que posi fi a la possessió i ús de les dades. És a dir, exigint del titular del fitxer que l'informi de quines dades posseeix sobre la seva persona, tot accedint als seus oportuns registres i assentaments, i quin destí han tingut, la qual cosa afecta també possibles cessionaris; i, si escau, requerir-lo perquè els rectifiqui o els cancel·li (FJ 7).

De manera que, privada la persona d'aquelles facultats de disposició i control sobre les seves dades personals, ho estarà també del seu dret fonamental a la protecció de dades, ja que, com va concloure en aquest punt la STC 11/1981, de 8 d'abril (FJ 8) s'ultrapassa o es desconeix el contingut essencial quan el dret queda sotmès a limitacions que el fan impracticable, el dificulten més enllà d'allò raonable o el desposseeixen de la necessària protecció (FJ 10).

El TC ha asseverat de manera rotunda com a contingut essencial d'aquest dret fonamental el dret d'informació de l'interessat. Evidentment, l'individu no pot controlar què es fa amb les seves dades si no sap que la seva dada la té un tercer i la pot utilitzar. Per tant, és capital per a l'efectiva garantia i respecte del dret tenir informat l'afectat de qui té les seves dades, per a què i amb quina finalitat, a l'efecte de conèixer el possible destí que pot donar-se a les seves dades personals. A més a més, aquest coneixement permet que l'afectat pugui reaccionar enfront de l'obtenció i ús de les seves dades exercint els drets d'oposició al tractament i de rectificació i cancel·lació de les dades.

La STC 292/2000 (FJ 13) subratlla que:

De manera que, sense la garantia que suposa el dret a una informació apropiada mitjançant el compliment de determinats requisits legals (art. 5 LOPD), quedaria sens dubte frustrat el dret de l'interessat a controlar i disposar de les seves dades personals, perquè és clar que li impedirien exercir altres facultats que s'integren en el contingut del dret fonamental a què fem referència.

Aquest contingut essencial del dret fonamental té eficàcia directa. És a dir, s'aplica directament a qualsevol relació o situació jurídica en què s'emprin dades personals. És igual que sigui la captació per una càmera de la imatge o del so d'un individu; en ambdós casos ja hem vist que es tracta de *dades personals* perquè permeten la identificació de la persona. Per tant, és indiferent que sigui l'enregistrament d'una conversa o el coneixement del llistat de trucades fetes o rebudes des d'un telèfon mòbil o l'enregistrament o obtenció d'imatges d'una persona o persones, tot això són dades personals i estan subjectes a aquest conjunt de garanties que componen el contingut essencial del dret fonamental a la protecció de dades que ha definit el TC, en especial en la seva Sentència 292/2000.

3. Les línies mestres de la protecció de dades. Qualitat de les dades i principis generals de la seva protecció

Aquest contingut constitucional s'ha desenvolupat per la LOPD, i també per la Directiva comunitària 95/46/CE, tot fixant, d'una banda, la «qualitat de les dades» i els principis generals que han de regir-ne la garantia i respecte.

L'article 4 LOPD, traslladant la Directiva 95/46/CE, fixa els criteris que defineixen la «qualitat» de les dades, o, per ser més exactes, l'estàndard lícit del tractament de les dades personals. En el que ara ens interessa, les dades personals consistents en imatges o en informacions digitals «només es podran recollir per al seu tractament, així com sotmetre-les a aquest tractament, quan siguin adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'hagin obtingut». No cal emprar les dades «per a finalitats incompatibles amb aquelles per a les quals les dades haguessin estat recollides», amb l'excepció de tractaments amb fins històrics, estadístics o científics. Convé en això recordar que la jurisprudència de l'Audiència Nacional ha variat de forma substancial l'entesa de què s'ha de considerar un fi incompatible. Al seu parer, només hi ha compatibilitat entre fins similars. Així doncs, es torna al criteri originari de la legislació anterior a la LOPD, en la qual, com ara per obra de l'Audiència Nacional, no hi ha tractaments de dades per a fins distints, encara que siguin compatibles, amb els originàriament expressats al mateix temps de l'obtenció de les dades.

El precepte fixa també els següents principis, que literalment es transcriuen del precepte citat:

1. Les dades de caràcter personal seran exactes i posades al dia de manera que responguin amb veracitat a la situació actual de l'afectat.
2. Si les dades de caràcter personal registrades resultessin inexactes, en tot o en part, o incompletes, seran cancel·lades i substituïdes d'ofici per les corresponents dades rectificades o completades.
3. Les dades de caràcter personal seran cancel·lades quan hagin deixat de ser necessàries o pertinents per a la finalitat per a la qual haguessin estat demanades o registrades. No seran conservades en forma que permeti la

identificació de l'interessat durant un període superior al necessari per als fins per als quals haguessin estat demanades o registrades.
4. Les dades de caràcter personal seran emmagatzemades de manera que permetin l'exercici del dret d'accés, tret que siguin legalment cancel·lades.
5. Es prohibeix la recollida de dades per mitjans fraudulents, deslleials o il·lícits.

La LOV, en l'article 6, estableix els «principis d'utilització de les videocàmeres», que, en gran manera, es compaginen amb els criteris de «qualitat de les dades» abans descrits i que, complementats per aquests últims, donarien cobertura sobrada a l'ús de sistemes de videovigilància des de la perspectiva del dret fonamental a la protecció de les dades personals.[4]

No hi ha dubte que el *principi de finalitat* és la clau de volta del sistema. La identificació precisa i coneguda dels propòsits perseguits en el tractament de les dades personals, també de les imatges que permetin identificar la persona o les seves comunicacions electròniques, és l'ancoratge a què s'uneixen els principis d'informació i consentiment, dels quals es parlarà més avall, i que constitueixen les tres línies mestres del règim de la protecció de les dades personals. Tant per a les agències, estatal i autonòmiques, de protecció de dades com per a la jurisprudència, es vulnera el dret a la protecció de dades si no es deixa ben clar a l'afectat per a què es volen aquestes dades i si això no es diu amb un cert grau de precisió o de concreció. El rebuig a l'utilització de finalitats genèriques impedeix acudir als «fins constitucionalment legítims» de l'activitat de les FFCCSS per justificar així el tractament de dades personals. No n'hi ha prou, per tant, amb la citació genèrica de l'article 104 CE (protegir el lliure exercici dels drets i llibertats i la seguretat ciutadana); s'ha de precisar quin motiu o finalitat concreta s'està perseguint amb aquesta activitat policial en què es demanen dades personals. No es pot justificar, sense més ni més, la captació d'imatges d'una persona al·legant raons de seguretat pública o de defensa nacional o la prevenció i persecució dels delictes. Tot això va unit a la idea d'inequívoc, és a dir, no pot haver-hi ambigüitats en la definició de les finalitats. Aquestes han de ser molt clares, de tal manera que l'afectat entengui perfectament i sigui conscient de la finalitat a què dedicaran les dades que se li demanen o que ja s'han obtingut.

---

4. *Principis d'utilització de les videocàmeres.* 1. La utilització de videocàmeres estarà presidida pel principi de proporcionalitat, en la seva doble versió d'idoneïtat i d'intervenció mínima. 2. La idoneïtat determina que només podrà emprar-se la videocàmera quan resulti adequat, en una situació concreta, per al manteniment de la seguretat ciutadana, de conformitat amb allò que s'ha disposat en aquesta llei. 3. La intervenció mínima exigeix la ponderació, en cada cas, entre la finalitat pretesa i la possible afectació per la utilització de la videocàmera al dret a l'honor, a la pròpia imatge i a la intimitat de les persones. 4. La utilització de videocàmeres exigirà l'existència d'un raonable risc per a la seguretat ciutadana, en el cas de les fixes, o d'un perill concret, en el cas de les mòbils. 5. No es podran utilitzar videocàmeres per obtenir imatges ni sons de l'interior dels habitatges, ni dels seus vestíbuls, llevat del consentiment del titular o autorització judicial, ni dels llocs inclosos en l'article 1 d'aquesta llei quan s'afecti de forma directa i greu la intimitat de les persones, així com tampoc per enregistrar converses de naturalesa estrictament privada. Les imatges i sons obtinguts accidentalment en aquests casos hauran de ser destruïts immediatament per qui tingui la responsabilitat de la seva custòdia.

D'altra banda, i prova de la importància del principi de finalitat i la seva estricta observança, l'ús i cessió de les dades per al mateix tipus de fi exigeix únicament el consentiment inicial manifestat al mateix temps de la recollida. Aquest consentiment prestat per a l'ús de les dades amb un fi determinat i explícit s'estén també a usos posteriors de les dades, fins i tot als derivats de cessions a tercers, sempre que aquests usos persegueixin un fi similar (això és, que no sigui distint) al que va justificar-ne la recollida i del qual va ser informat l'afectat en aquell moment.[5]

L'ús d'aquestes dades suscita majors qüestions per a fins distints, però compatibles, amb els que van justificar-ne la recollida. En aquest cas, la compatibilitat de fins faria lícita la cessió de les dades, segons disposa l'article 11.2 LOPD, però exigeix un nou i específic consentiment sobre la nova finalitat perseguida amb l'ús d'aquelles. Per descomptat, la LOPD veda l'ús de les dades personals per a fins diferents dels que van motivar-ne la recollida, tot exigint, si es pretén utilitzar-les d'aquesta manera, la posada en coneixement a l'interessat del nou destí de les seves dades i l'obtenció del seu consentiment perquè així sigui. La STC 292/2000 ha estat meridiana en aquest extrem: «... la cessió de les mateixes (es refereix a les dades) a un tercer per tal de procedir a un tractament amb fins diferents dels que van originarne la recollida, encara que siguin compatibles amb aquests (art. 4.2), suposa una nova possessió i ús que requereix el consentiment de l'interessat».

És cert que la LOPD parla de fins «incompatibles», la qual cosa inicialment va ser entesa com l'autorització legal perquè les dades es destinessin a fins diferents dels que van encoratjar-ne la recollida sense que fos necessari un nou consentiment de l'afectat sempre que aquests fins fossin compatibles amb els de l'obtenció de les dades. No obstant això, les Sentències de l'Audiència Nacional, Sala del Contenciós Administratiu, de 8 de febrer de 2002 i 11 de desembre de 2004, amb suport en la STC 292/2000, han refermat que malgrat la dicció literal de l'article 4 LOPD, els fins de recollida i de cessió han de ser similars, no n'hi ha prou amb la compatibilitat, per entendre que el consentiment donat per l'afectat perquè les seves dades fossin recollides per a un fi també s'estén a les cessions que se'n faci a tercers.

Convé tenir en compte també que la Sentència del Tribunal Suprem, Sala Tercera, de 15 d'abril de 2002, afirma, en aplicació de la STC 292/2000, que la cessió o comunicació de dades entre administracions públiques per assolir precisament el fi o un dels fins a què va obeir la recollida de la dada, no requereix reiterar el consentiment prestat en el moment de la recollida. En aquestes línies, l'Agència de Protecció de Dades ha mantingut en les seves resolucions que, havent-hi identitat de fins entre els comunicats a l'interessat per demanar-li les dades i els perseguits pel cessionari, no cal consentir novament respecte de la cessió, ja que n'hi ha prou amb el consentiment prestat inicialment i que tàcitament s'estén a les cessions posteriors, és a dir, a l'accés a aquestes dades per part de tercers. En aquests supòsits, diu l'Agència, no s'infringeix l'article 11; malgrat que no s'hagi demanat un nou consentiment per a la cessió.

5. De fet, l'Agència de Protecció de Dades considera que el consentiment a un tractament per a un fi determinat s'estén tàcitament a les cessions que persegueixin idèntica finalitat.

Justament el que això sigui així deriva de l'exigència que el fi del tractament o la cessió sigui explícit i específic. Només així, només si l'afectat va poder conèixer amb precisió el fi o fins perseguits amb l'ús de les seves dades, es pot presumir el tàcit consentiment a la cessió de les seves dades a tercers per aconseguir les mateixes finalitats.

Cal ara abordar els principis d'informació i consentiment que tanquen el sistema de tutela del dret fonamental a la protecció de les dades personals.

Així, l'article 5 LOPD descriu quines informacions cal donar a l'individu per obtenir i tractar les seves dades. Fonamentalment, la informació es refereix a quines dades són d'obligat subministrament o quines conseqüències té el fet que hom es negui a donar aquestes dades. Cal informar-lo per a què es volen les dades i quin pot ser-ne el possible destí, és a dir, les cessions a tercers. Per tant, s'ha d'informar dels usos finals que pugui tenir aquesta informació, qui tindrà aquestes dades, on estaran dipositades i davant de qui he d'exercir els meus drets d'accés o possessió, rectificació i cancel·lació de les dades.

Essencialment, aquesta és la informació bàsica que hem d'oferir a aquella persona les dades de la qual estiguem utilitzant. Aquesta informació pot donar-se amb posterioritat a l'obtenció i tractament de les dades. És possible que, per raons que ja es veuran, les dades siguin obtingudes sense que en tingui coneixement la persona a qui es refereixen; cosa molt habitual, per cert, en l'activitat policial. Ara bé, això no excusa que en un moment determinat del procediment tinguem l'obligació d'informar-lo d'aquesta circumstància i que aquesta informació (i el posterior consentiment, si escau) sigui condició indispensable per a la licitud de l'ocupació d'aquestes dades a l'efecte probatori. Diu l'apartat 5 de l'article 5 LOPD: «Quan les dades de caràcter personal no hagin estat obtingudes de l'interessat, aquest haurà de ser informat de forma expressa, precisa i inequívoca, pel responsable del fitxer o el representant, durant els tres mesos següents al moment del registre de les dades, llevat que ja hagués estat informat amb anterioritat del contingut del tractament, de la procedència de les dades, així com d'allò que s'ha previst en les lletres a), d) i e) de l'apartat 1 del present article». Aquest serà el cas en la majoria de les ocasions en què es prenguin imatges per les FFCCSS. Per la seva banda, la LOV, en l'article 9, desenvolupat en l'article 21 del Reial Decret 596/1999, de 16 d'abril (i Annex), cobreix part d'aquesta informació, malgrat que resulta necessari complementar-la amb el que disposa el citat article 5 LOPD.

El principi del consentiment constitueix un altre element capital de la protecció de dades. Principi que regeix amb caràcter general, llevat de les excepcions expressament previstes en la LOPD (arts. 6, 11 i 21 LOPD), així com en la LOV. Cal demanar prèviament el consentiment de l'interessat per poder obtenir i utilitzar-ne les dades. Sense aquest consentiment, l'obtenció i ús de les dades resulten contraris al dret fonamental i, per tant, nuls. Cal pensar en la utilització com a prova en un procés penal de dades personals obtingudes mitjançant la captació d'imatges per un sistema de videovigilància. Si no s'acredita que les dades personals es van obtenir amb consentiment previ i informat de l'afectat o no s'acredita que es compleix alguna de les excepcions previstes en els articles 6, 11 o 21 LOPD, aquesta prova ha de qualificar-se d'il·lícita i prohibida per la lesió del dret fonamental a la

protecció de les dades personals, amb la qual cosa se'n perd la validesa com a prova de càrrec.

No s'han de perdre de vista d'altres deures genèrics previstos en la LOPD, que, no sent part integrant del contingut del dret fonamental, la seva inobservança pot ser motiu de sanció administrativa i podria suposar la declaració com a irregular de la prova obtinguda amb infracció dels esmentats deures. Aquests deures són tres: inscripció dels fitxers de dades en el Registre que depèn de l'Agència Espanyola de Protecció de Dades, el deure de secret i confidencialitat de l'article 10 LOPD, i, finalment, els deures relatius a les mesures de seguretat de l'article 9 LOPD.

Cal tenir en compte que, d'acord amb el Reglament de Seguretat encara vigent, Reial decret 944/1994, d'11 de juny, tots els fitxers relatius a dades en matèria d'infraccions penals o administratives estan considerats com de *seguretat alta* (art. 4 RD 944/1994).[6] S'ha de posar esment també que els fitxers policials, si bé tenen un règim específic, han de ser objecte d'inscripció en el Registre General a l'Agència de Protecció de Dades, i, a més a més, en el cas de FFCCSS autonòmiques o locals, a les agències autonòmiques de protecció de dades, si n'hi hagués. Més endavant veurem les peculiaritats que la pròpia LOPD en l'article 22 preveu per al cas dels fitxers amb fins policials. Respecte del deure de secret de l'article 10 LOPD, aquest ja estaria genèricament previst per al cas de les actuacions de les FFCCSS en l'article 5.5 de la Llei orgànica 2/1986, de 13 de març, de FFCCSS, i que en allò que ara interessa es veu reflectit en l'apartat 2 de l'article 8 LOV.

4. Els drets dels interessats

L'article 2 LOPD exclou del seu àmbit d'aplicació els fitxers sotmesos a la normativa sobre protecció de matèries classificades i els fitxers establerts per a la investigació del terrorisme i de formes greus de delinqüència organitzada.[7] A més a més, sotmet a la seva legislació específica «els procedents d'imatges i sons obtinguts mitjançant la utilització de videocàmeres per les forces i cossos de seguretat,

6. «1. Tots els fitxers que continguin dades de caràcter personal hauran d'adoptar les mesures de seguretat qualificades com de nivell bàsic. 2. Els fitxers que continguin dades relatives a la comissió d'infraccions administratives o penals, Hisenda Pública, serveis financers i aquells fitxers el funcionament dels quals es regeixi per l'article 28 de la Llei orgànica 5/1992, hauran de reunir, a més de les mesures de nivell bàsic, les qualificades com de nivell mitjà. 3. Els fitxers que continguin dades d'ideologia, religió, creences, origen racial, salut o vida sexual, així com els que continguin dades demanades per a fins policials sense consentiment de les persones afectades, hauran de reunir, a més de les mesures de nivell bàsic i mitjà, les qualificades com de nivell alt. 4. Quan els fitxers continguin un conjunt de dades de caràcter personal suficients que permetin obtenir una avaluació de la personalitat de l'individu hauran de garantir les mesures de nivell mitjà establertes en els articles 17, 18, 19 i 20. 5. Cadascun dels nivells descrits anteriorment tenen la condició de mínims exigibles, sense perjudici de les disposicions legals o reglamentàries específiques vigents.»

7. El propi precepte assenyala que: «No obstant això, en aquests supòsits el responsable del fitxer comunicarà prèviament l'existència d'aquest, les seves característiques generals i la seva finalitat a l'Agència de Protecció de Dades». Això no suposa la seva inscripció en el Registre de l'Agència, sinó la comunicació de la seva existència.

de conformitat amb la legislació sobre la matèria»; és a dir, la LOV. No obstant això, aquestes exclusions no comporten una no subjecció a les garanties derivades del contingut constitucional del dret fonamental a la protecció de dades. En el cas de la videovigilància es produeix una peculiar remissió inversa, per tal com l'apartat 2 del seu article 2 remet al que disposa la legislació de protecció de dades que en l'actualitat és la LOPD. Per tant, pel que fa al cas, el règim de protecció de dades en matèria de videovigilància és l'establert amb caràcter general en la LOPD, malgrat el que disposa la pròpia LOPD.

Un aspecte important és el relatiu als drets dels interessats enfront del tractament de les dades personals. La LOPD desenvolupa aquests drets, concretant el contingut constitucional del dret fonamental, que al seu torn tenen una ulterior concreció en el Reial Decret 1332/1994, de 20 de juny (complementada amb la Instrucció 1/1998 de l'Agència Espanyola de Protecció de Dades). Aquests drets són: a la informació (art. 5), a consentir (art. 6), d'accés (art. 15), de rectificació i cancel·lació (art. 16), i d'oposició (arts. 6 i 30). D'ordre legal són els drets a la impugnació de valoracions (art. 13), de consulta del Registre (art. 14) i a indemnització (art. 19).

Aquests mateixos drets també es contemplen en la normativa especificada de videovigilància, com recorden tant la LOV com el seu Reglament de desplegament, Reial Decret 596/1999, de 16 d'abril (en endavant, RV), que regulen els drets d'informació, accés i cancel·lació dels interessats («ciutadans», diu el RV en el seu capítol V) respecte de les imatges, de les dades obtingudes amb ocasió de la captació d'imatges i so, per la instal·lació de càmeres fixes, o per l'ús de les càmeres mòbils.

No obstant això, no es contempla ni el dret d'impugnació de les valoracions, ni el dret de consulta del Registre General de l'Agència de Protecció de Dades. Tampoc no contempla els drets a consentir i d'oposició a l'ús i tractament de les dades personals així captades. Tanmateix, en la mesura que el propi article 2.2 LOV remet a la LOPD, cal entendre que en aquesta matèria també s'apliquen aquests preceptes de la LOPD que han estat citats. Per tant, el règim de consentiment o oposició i de consulta al Registre general podria ampliar-se també al registre d'enregistraments obtinguts per mitjà de la videovigilància, exercint-se en els termes que preveu la LOPD, el Reial Decret 1332/1994, la Instrucció de l'Agència de Protecció de Dades 1/1998, i en el que, sobre el particular, hagin disposat les agències de protecció de dades autonòmiques en el cas que hagin establert alguna especificitat en els procediments.

Les excepcions als drets de les persones constitueixen un afer de primer ordre. Cal portar aquí les reflexions realitzades per la STC 292/2000. En primer lloc, l'article 23 LOPD estableix un elenc important d'excepcions del dret dels usuaris en el cas dels fitxers de titularitat pública, per tant, també als fitxers utilitzats per les FFCCSS (que tenen els seus propis), que, en general, estan tots fonamentats en béns o interessos de rang constitucional.

Diu aquest article 23:

> 1. Els responsables dels fitxers que continguin les dades a què es refereixen els apartats 2, 3 i 4 de l'article anterior (que és l'article 22) podran denegar l'accés, la rectificació o cancel·lació en funció dels perills que poguessin derivar-se per a la de-

> fensa de l'Estat o la seguretat pública, la protecció dels drets i llibertats de tercers o les necessitats de les investigacions que s'estiguin realitzant.
>
> 2. Els responsables dels fitxers de la Hisenda Pública podran, igualment, denegar l'exercici dels drets a què es refereix l'apartat anterior quan aquell obstaculitzi les actuacions administratives tendents a assegurar el compliment de les obligacions tributàries i, en tot cas, quan l'afectat sigui objecte d'actuacions inspectores.
>
> 3. L'afectat a qui es denegui, totalment o parcial, l'exercici dels drets esmentats en els apartats anteriors podrà posar-ho en coneixement del director de l'Agència de Protecció de Dades o de l'organisme competent de cada Comunitat Autònoma en el cas de fitxers mantinguts per cossos de policia propis d'aquestes, o per les administracions tributàries autonòmiques, els quals hauran d'assegurar-se de la procedència o improcedència de la denegació.

Cal aclarir que, arran de la doctrina del TC assentada en la citada STC 292/2000, la *seguretat pública* a què es fa esment en l'apartat 1 d'aquest article 23 i que permetria excepcional els drets dels interessats en el cas de fitxers de les FFCCSS, inclosos els formats amb els enregistraments obtinguts pels sistemes de videovigilància, caldria entendre-la cenyida exclusivament a la prevenció i persecució de les infraccions penals.

Així hauria de ser, segons la nostra opinió, com a conseqüència de la declaració d'inconstitucionalitat d'alguns incisos dels apartats de l'article 24 LOPD. Aquest precepte estableix que:

> 1. El que disposen els apartats 1 i 2 de l'article 5è (drets d'informació) no serà aplicable a la recollida de dades quan la informació a l'afectat impedeixi o dificulti greument *el compliment de les funcions de control i verificació de les administracions públiques* o quan afecti la Defensa Nacional, la seguretat pública o la persecució d'infraccions penals *o administratives*.
>
> 2. Allò que disposa l'article 15 (dret d'accés) i l'apartat 1 de l'article 16 (drets de rectificació i cancel·lació) no s'aplicarà si, sopesats els interessos en presència, resultés que els drets que els esmentats preceptes concedeixen a l'afectat haguessin de cedir davant raons d'*interès públic o davant interessos de tercers més dignes de protecció*. Si l'òrgan administratiu responsable del fitxer invoqués allò que s'ha disposat en aquest apartat, dictarà una resolució motivada i instruirà l'afectat del dret que l'assisteix a posar la negativa en coneixement del director de l'Agència de Protecció de Dades o, si escau, de l'òrgan equivalent de les comunitats autònomes.

El TC va considerar que els incisos en cursiva eren una habilitació en blanc a l'Administració pública per decidir amb un grau intolerable de discrecionalitat en quins casos dóna curs a l'exercici dels drets dels usuaris i en quins casos no amb el fàcil expedient d'acudir a aquelles excuses genèriques. En aquest punt el TC ha estat molt contundent. En els FFJJ 17 i 18 del seu STC 292/2000 va afirmar:

17. En el cas present, l'ocupació per la LOPD en el seu article 24.1 de l'expressió «funcions de control i verificació» obre un espai d'incertesa tan ampli que provoca una doble i perversa conseqüència. D'una banda, en habilitar la LOPD a l'Administració perquè restringeixi drets fonamentals invocant tal expressió està renunciant a fixar ella mateixa els límits, tot donant poders a l'Administració per fer-ho. I d'una manera tal que, com assenyala el Defensor del Poble, permet reconduir a aquelles pràcticament tota activitat administrativa, ja que tota activitat administrativa que impliqui entaular una relació jurídica amb un administrat, que així serà pràcticament en tots els casos en què l'Administració necessiti dades personals d'algú, comportarà d'ordinari la potestat de l'Administració de verificar i controlar que aquest administrat ha actuat conforme al règim jurídic administratiu de la relació jurídica entaulada amb l'Administració. La qual cosa, a la vista del motiu de restricció del dret a ser informat de l'article 5 LOPD, deixa en la més absoluta incertesa el ciutadà sobre en quins casos concorrerà aquesta circumstància (si no en tots) i sumeix en la ineficàcia qualsevol mecanisme de tutela jurisdiccional que hagi d'enjudiciar tal supòsit de restricció de drets fonamentals sense cap més criteri complementari que vingui en ajuda del seu control de l'actuació administrativa en aquesta matèria.

Els mateixos retrets mereix, així mateix, la utilització en l'article 24.2 LOPD de l'expressió «interès públic» com a fonament de la imposició de límits als drets fonamentals de l'article 18.1 i 4 CE, ja que inclou un grau d'incertesa encara més gran. Només cal tenir en compte que tota activitat administrativa, en últim terme, persegueix la salvaguarda d'interessos generals, la consecució de la qual constitueix la finalitat a què ha de servir amb objectivitat l'Administració d'acord amb l'article 103.1 CE.

18. Les mateixes recusacionss mereixen també els altres dos casos de restriccions que han estat impugnats pel Defensor del Poble, la relativa a la persecució d'infraccions administratives (art. 24.1 LOPD) i la garantia d'interessos de tercers més dignes de protecció (art. 24.2 LOPD).

L'interès públic per sancionar infraccions administratives no resulta, en efecte, suficient, com s'evidencia que ni tan sols es preveu com a límit per al simple accés als arxius i registres administratius contemplats en l'article 105.b) CE. Per la qual cosa, la possibilitat que, d'acord amb l'article 24.1 LOPD, l'Administració pugui sostreure a l'interessat informació relativa al fitxer i les seves dades segons disposa l'article 5.1 i 2 LOPD, tot invocant els perjudicis que tal informació pugui ocasionar a la persecució d'una infracció administrativa, suposa una greu restricció dels drets a la intimitat i a la protecció de dades mancada de fonament constitucional. I cal observar que es tracta, a més a més, d'una pràctica que pot causar greu indefensió en l'interessat, que pot veure's impedit d'articular adequadament la seva defensa enfront d'un possible expedient sancionador per la comissió d'infraccions administratives, en negar-li la pròpia Administració accés a les dades que sobre la seva persona pugui posseir i que puguin ser emprades en contra seu sense possibilitat de cap defensa en no poder rebatre-les pel fet de resultar-li ignotes a l'afectat. La pròpia LOPD estableix en el seu article 13 que els ciutadans «tenen dret a no veure's sotmesos a una decisió amb efectes jurídics, sobre ells o que els afecti de manera significativa, que es basi únicament en un tractament de dades destinades

a avaluar determinats aspectes de la seva personalitat». Criteris difícilment compatibles amb la denegació del dret a ser informat de l'article 5 LOPD acordada per l'Administració pública amb l'únic fonament de la persecució d'una infracció administrativa.

Per últim, l'apartat 2 de l'article 24 LOPD estableix que els drets d'accés a les dades (art. 15.1 i 2 LOPD) i els de rectificació i cancel·lació d'aquestes (art. 16.1 LOPD) podran denegar-se també si, «ponderats els interessos en presència, resultés que els drets que els esmentats preceptes concedeixen a l'afectat haguessin de cedir davant [...] interessos de tercers més dignes de protecció». Resulta evident que, després del que ja s'ha dit, a la vista que aquest incís permet al responsable del fitxer públic negar a un interessat l'accés, rectificació i cancel·lació de les seves dades personals, i al marge que aquests interessos puguin identificar-se amb els drets fonamentals d'aquest tercer o amb qualsevol altre interès que pogués esgrimir-se, tal negativa implica abandonar a la decisió administrativa la fixació d'un límit al dret fonamental a la protecció de les dades de caràcter personal sense ni tan sols establir quins puguin ser aquests interessos ni les circumstàncies en què calgui fer-los valer per restringir d'aquesta forma aquest dret fonamental.

[…]

Com en una altra ocasió hem asseverat, els motius de limitació acusen un tal grau d'indeterminació que deixen excessiu camp de maniobra a la discrecionalitat administrativa, incompatible amb les exigències de la reserva legal atès que constitueix una cessió en blanc del poder normatiu que defrauda la reserva de llei. A més a més, en no fer cap referència als pressupòsits i condicions de la restricció, resulta insuficient per determinar si la decisió administrativa és o no el fruit previsible de la raonable aplicació del que disposa el legislador (SSTC 101/1991, FJ 3, i 49/1999, FJ 4). De manera que la mateixa falta evident de certesa i previsibilitat del límit que l'article 24.2 LOPD imposa al dret fonamental a la protecció de les dades personals (art. 18.4 CE), i la circumstància que, a més a més, es tracti d'un límit la fixació i aplicació del qual no ve precisada en la LOPD, sinó que es lliura a la total discreció de l'Administració pública responsable del fitxer en qüestió, i condueix a l'estimació en aquest punt del recurs interposat pel Defensor del Poble en resultar vulnerats els articles 18.4 i 53.1 CE.

Això té certa importància perquè una clàusula molt similar està prevista en la LOV respecte a les restriccions que el responsable d'aquests fitxers pot oposar a l'exercici dels drets d'accés i cancel·lació dels afectats per un control de videovigilància. L'article 9 LOV disposa que podra denegar-se l'exercici d'aquests drets «en funció dels perills que se'n poguessin derivar per a la defensa de l'Estat, la seguretat pública, la protecció dels drets i llibertats de tercers o les necessitats de les investigacions que s'estan realitzant». Sembla que, en una recta aplicació de la doctrina abans transcrita de la STC 292/2000, caldria considerar contrari al dret fonamental a la protecció de dades la denegació de l'exercici dels drets citats si el motiu de la denegació consisteix en la protecció de «les necessitats de les investigacions que s'estiguin realitzant», i res més.

5. Les peculiaritats dels fitxers policials. L'article 22 LOPD

L'article 22 LOPD estableix:

> 1. Els fitxers creats per les Forces i Cossos de Seguretat que continguin dades de caràcter personal que, pel fet d'haver-se recollit per a fins administratius, hagin de ser objecte de registre permanent, estaran subjectes al règim general d'aquesta llei.
>
> 2. La recollida i tractament per a fins policials de dades de caràcter personal per les Forces i Cossos de Seguretat sense consentiment de les persones afectades estan limitats a aquells supòsits i categories de dades que resultin necessaris per a la prevenció d'un perill real per a la seguretat pública o per a la repressió d'infraccions penals, per a la qual cosa han de ser emmagatzemats en fitxers específics establerts a aquest efecte, que hauran de classificar-se per categories en funció del seu grau de fiabilitat.
>
> 3. La recollida i tractament per les Forces i Cossos de Seguretat de les dades, a què fan referència els apartats 2 i 3 de l'article 7è, podran realitzar-se exclusivament en els supòsits en què sigui absolutament necessari per als fins d'una investigació concreta, sense perjudici del control de legalitat de l'actuació administrativa o de l'obligació de resoldre les pretensions formulades, si escau, pels interessats que corresponen als òrgans jurisdiccionals.
>
> 4. Les dades personals registrades amb fins policials es cancel·laran quan no siguin necessàries per a les investigacions que van motivar-ne l'emmagatzemament.
>
> A aquest efecte, es considerarà especialment l'edat de l'afectat i el caràcter de les dades emmagatzemades, la necessitat de mantenir les dades fins a la conclusió d'una investigació o procediment concret, la resolució judicial ferma, en especial l'absolutòria, l'indult, la rehabilitació i la prescripció de responsabilitat.

Aquest ha de ser, al nostre parer, el marc general dels fitxers que continguin imatges obtingudes per mitjà de sistemes de videovigilància, atès que els fins de l'ús de sistemes de videovigilància són similars als que, d'acord amb el citat article, permetrien l'existència de fitxers de les FFCCSS (art. 1 LOV). Deixant de banda la impossibilitat de la «rectificació» d'aquest tipus de dades, no se'ns acut quina qualitat podria fer d'aquest tipus de font de dades personals un mecanisme per a la seva obtenció i tractament aliè al que disposa la LOPD, i més en concret, del seu article 22.

5.1 Tipologia de fitxers policials

La LOPD, en l'article 22, distingeix, segons sembla, entre els fitxers policials amb finalitats administratives i aquells utilitzats per a «fins policials», diu la norma, i que haurien d'entendre's referits a investigacions de fets que poguessin ser constitutius d'infraccions penals i/o administratives.

Els fitxers policials que tenen finalitat administrativa són tractats com qualsevol altre fitxer de qualsevol altra Administració pública. Aquests fitxers estan subjectes al règim general de la LOPD.

Els fitxers amb finalitats policials que regula l'article 22.2 LOPD s'han de classificar en aquells on hi ha hagut un previ consentiment de l'afectat perquè les seves dades siguin incorporades a aquest fitxer i sotmeses a tractament, i aquells en què no hi ha aquest previ consentiment, i, en conseqüència, no hi ha coneixement per part de l'afectat de la seva recollida i tractament ni prèvia informació. Aquests últims són els que expressament regula l'apartat 2 de l'article 22. Diu aquest apartat segon:

> 2. La recollida i tractament per a fins policials de dades de caràcter personal per les Forces i Cossos de Seguretat sense consentiment de les persones afectades estan limitats a aquells supòsits i categories de dades que resultin necessàries per a la prevenció d'un perill real per a la seguretat pública o per a la repressió d'infraccions penals, i han de ser emmagatzemades en fitxers específics establerts a aquest efecte, que hauran de classificar-se per categories en funció del seu grau de fiabilitat.

Llavors, cal induir de l'article 22 LOPD que tot tractament de dades efectuat per les FFCCSS que persegueixi fins administratius, o amb fins policials que no estiguin lligats a «la prevenció d'un perill real per a la seguretat pública o per a la repressió d'infraccions penals» estan subjectes al règim general de la LOPD.

Tenint en compte el que s'ha dit més amunt, respecte dels drets dels interessats, el cas dels fitxers amb fins policials que poden crear-se i existir sense previ consentiment de l'interessat, i, en conseqüència, sense estar informat sobre la seva existència i finalitat, planteja seriosos dubtes quan es tracta de procediments administratius (cal pensar en el règim d'estrangers). Menys dubtes plantegen, al contrari, els que es creïn en el marc d'investigacions policials concretes dins una instrucció penal.

Segons la nostra opinió, els fitxers, temporals o permanents[8] que resultin de l'ús de videocàmeres fixes o mòbils s'ha d'enquadrar en el marc de l'article 22 LOPD, atesa, d'altra banda, la coincidència de fins. L'article 1 LOV disposa que l'objecte d'aquesta llei és regular «la utilització per les Forces i Cossos de Seguretat de videocàmeres per enregistrar imatges i sons en llocs públics, oberts o tancats, i el seu posterior tractament, a fi de contribuir a assegurar la convivència ciutadana, l'eradicació de la violència i la utilització pacífica de les vies i espais públics, així

8. Cal no oblidar que la LOV preveu un règim específic de conservació dels enregistraments en l'article 8: «Els enregistraments seran destruïts en el termini màxim d'un mes des de la seva captació, llevat que estiguin relacionats amb infraccions penals o administratives greus o molt greus en matèria de seguretat pública, amb una investigació policial en curs o amb un procediment judicial o administratiu obert». Això és desenvolupat en detall pels articles 18, 19 i 20 RV. No es pot oblidar que conforme al que disposa l'apartat 4 de l'article 22 LOPD: «Les dades personals registrades amb fins policials es cancel·laran quan no siguin necessàries per a les investigacions que van motivar-ne l'emmagatzemament. A aquest efecte, es considerarà especialment l'edat de l'afectat i el caràcter de les dades emmagatzemades, la necessitat de mantenir les dades fins a la conclusió d'una investigació o procediment concret, la resolució judicial ferma, en especial l'absolutòria, l'indult, la rehabilitació i la prescripció de responsabilitat». Sens dubte, per tal de fixar l'abast temporal d'aquesta necessitat serà de gran utilitat la rica doctrina del TC sobre el temps de la detenció de l'article 17.2 CE.

com de prevenir la comissió de delictes, faltes i infraccions relacionats amb la seguretat publica». Això complementen els articles 4 i 5 LOV en establir els motius que poden justificar la instal·lació i/o ús de càmeres fixes i d'equips d'enregistrament mòbils. En el primer cas aquests motius són «assegurar la protecció dels edificis i instal·lacions públiques i dels seus accessos; salvaguardar les instal·lacions útils per a la defensa nacional; constatar infraccions a la seguretat ciutadana, i prevenir la causació de danys a les persones i béns»; i en el segon «per al millor compliment dels fins que preveu aquesta llei, quedant, en tot cas, supeditada l'obtenció, que ha de ser conjunta, d'imatge i so, a la concurrència d'un perill concret».

El propi article 22 contempla el cas d'aquells fitxers policials que continguin dades dels comunament denominats «sensibles» de l'article 7 LOPD: ideologia, religió o creences, afiliació sindical i els que facin referència a l'origen racial, a la salut i a la vida sexual.

En aquest cas, la LOPD acudeix a la doctrina del perill cert, real i imminent per justificar excepcionalment l'obtenció d'aquestes dades i el seu tractament per les FFCCSS. Estableix l'article 22, en el seu apartat 4, que la recollida i tractament de dades sensibles per les FFCCSS només podrà realitzar-se «en els supòsits en què sigui absolutament necessari per als fins d'una investigació concreta». Així doncs, podrà crear-se un fitxer policial, o podrà contenir aquest tipus de dades, si és possible acreditar l'existència d'un risc cert, imminent i real que en requereixi la utilització, l'evident formalització de la qual és l'existència d'una investigació concreta. No n'hi ha prou, doncs, amb la mera sospita, sinó que cal que hi hagi indicis racionals que hi ha aquest perill, i així s'haurà de raonar en el marc d'una investigació, sota pena d'infringir el principi de proporcionalitat (arts. 6 LOV i 4 LOPD). També aquest criteri s'ha d'aplicar a l'ús de videocàmeres (cal tenir en compte els enregistraments d'una manifestació pública en què després es pugui associar determinades persones amb determinades ideologies o filiacions sindicals o polítiques, com succeïa en el cas de la STC 37/1998, de la qual més avall es fan unes observacions).[9]

5.2 Creació dels fitxers i responsable del tractament

Els fitxers policials no estan exceptuats del règim general de creació, modificació i supressió de fitxers per les Administracions públiques (art. 20 LOPD). Per tant, la creació de fitxers per la policia amb ocasió de les seves activitats tant en la prevenció com en la persecució d'infraccions administratives o penals, i també els derivats de la videovigilància, estan subjectes a la prèvia existència d'una disposició de caràcter general que reguli l'existència, contingut, ús, destí, modificació i

9. No convé oblidar que l'article 55 CE relatiu a la suspensió general o singular de drets fonamentals no contempla el dret a la intimitat o a la protecció de dades. Amb caràcter general en aquesta matèria és de citació obligada la SSTC 199/1987 i 71/1994. I no s'oblidi que el propi article 2 LOPD exclou del seu àmbit allò relatiu a la lluita antiterrorista i contra la delinqüència organitzada.

forma de supressió del fitxer, en aquest cas del fitxer policial. I aquesta disposició no és la LOV o el RV, és clar. Si no hi ha aquesta norma de creació, aquest fitxer és contrari al dret fonamental a la protecció de dades.

La LOPD ha creat la figura del responsable del fitxer o del tractament que en defineix l'article 3.d) en els termes següents: «persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que decideixi sobre la finalitat, contingut i ús del tractament». Hi ha acord sobre el fet que aquesta figura no s'ha d'identificar amb el *propietari* del fitxer, sinó amb qui tingui atribuït el poder jurídic de disposició sobre aquell. En aquest sentit, la LOV identifica a qui hauria de tenir-se per responsable del fitxer o tractament derivat de l'ús de videocàmeres en l'article 8.4 en assenyalar: «reglamentàriament, l'administració competent determinarà l'òrgan o autoritat governativa que tindrà a càrrec seu la custòdia de les imatges obtingudes i la responsabilitat sobre el seu ulterior destí, inclosa la inutilització o destrucció. L'esmentat òrgan serà el competent per resoldre sobre les peticions d'accés o cancel·lació promogudes pels interessats».

Així definida aquesta «autoritat» respon amb meridiana claredat al responsable del fitxer o del tractament previst en la LOPD i sobre el qual pesen una sèrie d'obligacions ja descrites en aquest treball unes pàgines més amunt. Es podria suggerir la utilització de la norma reglamentària que la identifiqui per a establir, precisament, els termes de creació i ús del fitxer derivat de la utilització de videocàmeres, complint amb les previsions de l'article 20 LOPD, entre les quals figura justament la identificació del responsable (art. 20.1.f) LOPD).

5.3 Comunicació de dades contingudes en fitxers policials

L'article 21 LOPD afecta també aquesta matèria, ja que regula amb caràcter general els termes en què es poden cedir dades entre administracions públiques. Les regles de la cessió, és a dir, de la comunicació de dades entre administracions, per tant entre les diverses FFCCSS i d'aquestes amb altres ens públics, són: en primer lloc, que han d'estar previstes en la disposició general que reguli l'existència dels fitxers policials; en segon lloc, només pot haver-hi cessions no previstes en la disposició de creació del fitxer si les dades es comuniquen a una altra Administració pública per exercir competències similars o sobre la mateixa matèria que les exercides per l'Administració cedent, o ho preveu una norma amb rang de llei orgànica (STC 290/2000); en tercer lloc, les cessions han de ser conegudes i consentides per l'afectat; no obstant això, el consentiment previ de la persona les dades de la qual s'han de cedir només és necessari en el cas que se cedeixin per tal d'exercir competències distintes o sobre matèries diferents, si aquesta cessió no està prevista en la disposició general de creació del fitxer o en una norma amb rang de llei orgànica.[10]

10. Criteri que, al nostre parer, encaixaria en allò que disposa l'article 11 LOPD apartat a) (cessions autoritzades per llei) i d) («Quan la comunicació que hagi d'efectuar-se tingui per destinatari el Defensor del Poble, el Ministeri Fiscal o els jutges o tribunals o el Tribunal de Comptes, en l'exercici de les funcions que té atribuïdes. Tampoc no serà necessari el consentiment quan la comunicació tingui

En conseqüència, i advertits que els llocs de trànsit públic no són «fonts accessibles al públic»[11] que autoritzin una comunicació d'imatges de persones sense el seu consentiment (art. 11.b) LOPD), les FFCCSS només podran cedir sense el previ consentiment dels afectats els enregistraments i fitxers d'enregistraments d'imatges o sons obtinguts amb sistemes de videovigilància a altres administracions públiques si així està previst en la disposició general de creació del fitxer, que haurà de tenir en aquest cas rang de llei orgànica en tractar-se d'una restricció d'un dret fonamental (STC 290/2000); o si «l'Administració cessionària és el Defensor del Poble, el Ministeri Fiscal o els jutges o tribunals o el Tribunal de Comptes, en l'exercici de les funcions que té atribuïdes. Tampoc no serà necessari el consentiment quan la comunicació tingui com a destinatari institucions autonòmiques amb funcions anàlogues al Defensor del Poble o al Tribunal de Comptes» (art. 11.d) LOPD).[12]

Si bé l'apartat 3 de l'article 8 LOV prohibeix les cessions o còpies de les imatges i sons videoenregistrats, aquesta tan severa regla estableix les excepcions tot remetent al seu apartat 1, segons el qual els enregistraments podrien ser, en el que ara ens interessa, cedits si estan «relacionats amb infraccions penals o administratives greus o molt greus en matèria de seguretat pública, amb una investigació policial en curs o amb un procediment judicial o administratiu obert». Això es correspon amb el que disposa l'article 7 LOV.

En aquest sentit l'article 7 LOV regula la cessió de les dades derivades de la utilització de les videocàmeres de manera ajustada a les previsions de la LOPD. Aquest precepte estableix que si les imatges haguessin captat fets que poguessin tenir rellevància penal, seran comunicats a l'autoritat judicial o al Ministeri Fiscal. Aquesta cessió no requereix el consentiment previ dels afectats com així resulta de l'article 11.2.d) LOPD. L'article 7 en l'apartat 2 fa el mateix en el cas que els fets poguessin ser constitutius d'una infracció administrativa relacionada amb la seguretat ciutadana. En aquest cas, i amb tota cautela, es podria donar cobertura a aquesta cessió, i fins i tot podria tenir lloc sense el previ consentiment de l'afectat, aplicant allò que disposa l'article 21.1 i 4 LOPD; és a dir, se cedeixen dades per tal d'assolir els mateixos fins referits a la seguretat ciutadana que van motivar-ne la recollida (identitat de matèries i fins). Cal recordar que l'Agència estatal de Protecció de Dades considera que si hi ha identitat de fins entre els successius usos a què es destini la dada, només fa falta comptar amb el consentiment per a la primera utilització.

---

com a destinatari institucions autonòmiques amb funcions anàlogues al Defensor del Poble o al Tribunal de Comptes»).

11. Article 3.j) LOPD: «Fonts accessibles al públic: aquells fitxers la consulta dels quals pot ser realitzada, per qualsevol persona, no impedida per una norma limitadora o sense més exigència que, si escau, l'abonament d'una contraprestació. Tenen la consideració de fonts d'accés públic, exclusivament, el cens promocional, els repertoris telefònics en els termes previstos per la seva normativa específica i les llistes de persones pertanyents a grups de professionals que continguin únicament les dades de nom, títol, professió, activitat, grau acadèmic, adreça i indicació de la seva pertinença al grup. Així mateix, tenen el caràcter de fonts d'accés públic els diaris i butlletins oficials i els mitjans de comunicació.»

12. Al marge, és clar, de la comunicació de dades dissociades o amb fins històrics, científics o estadístics, article 11.e) i apartat 6.

Convé que ens detinguem un instant en la comunicació de dades entre unitats del mateix cos i entre diferents FFCCSS. En el primer cas, per manca de criteri jurisprudencial o de les agències de protecció de dades, semblaria que s'ha de considerar cessió quan l'accés a les dades s'autoritza a cossos o unitats de policia que no cal considerar integrats orgànicament i/o funcionalment en aquell que va obtenir les dades. Al nostre parer, la personalitat jurídica autònoma de la unitat o cos és el criteri que ha de permetre'ns distingir entre aquells que poden considerar-se una mateixa Administració pública i aquells que pertanyen a administracions distintes, de manera que només hi hauria cessió de dades en aquest segon cas.

La cooperació internacional en la lluita contra el terrorisme i les formes organitzades de delinqüència impliquen diverses formes de cessió de dades entre FFCCSS de diferents estats. Malgrat que potser no sigui aquest el lloc convenient per abordar aquest afer, indubtablement posseeix un relleu de primer ordre. D'una banda, per la intensitat i extensió de l'intercanvi de dades que comporta el Sistema d'Informació Schengen,[13] que no es limita a l'intercanvi de dades en matèria de terrorisme i bandes organitzades de delinqüències; i d'una altra, les necessitats derivades de la cooperació judicial i policial internacional. És l'última expressió d'aquest fenomen la recent i no menys polèmica Directiva 2006/24/CE del Parlament Europeu i el Consell, de 15 de març de 2006, sobre la conservació de dades generals o tractats en relació amb la prestació de serveis de comunicacions electròniques d'accés públic o de xarxes públiques de comunicacions i per la qual es modifica la Directiva 2002/58/CE.[14]

La LOPD regula en els seus articles 33 i 34, títol V, el moviment internacional de dades. Aquesta regulació es redueix a una norma molt simple: no es poden transferir dades obtingudes a Espanya a un altre estat, sigui un estat de la Unió Europea o no, sense que hi hagi una declaració del que es coneix com a «port segur». I per tals ha d'entendre's aquells «països que […] proporcionin un nivell de protecció equiparable al que presta aquesta llei, llevat que, a més d'haver-se observat allò que s'ha disposat en aquesta, s'obtingui autorització prèvia del director de l'Agència de Protecció de Dades, que només podrà atorgar-la si s'obtenen garanties adequades» (art. 33.1 LOPD).

Aquesta declaració se subjecta a un procediment reglat en el propi article 33 LOPD,[15] i que és competència de l'Agència Estatal de Protecció de Dades. L'article

13. Conscient d'això el legislador internacional, el Conveni d'aplicació de l'Acord de Schengen de 14 de juny de 1985, relatiu a la supressió gradual dels controls a les fronteres comunes (a què es va adherir Espanya per Acord de 25 de juny de 1991), dedica el seu capítol III (arts. 102 a 118) a la protecció de dades.

14. El seu article 7 es refereix a la «protecció i seguretat de les dades» amb una genèrica i una mica confusa remissió a la Directiva 95/46/CE i a la 2002/58/CE.

15. «El caràcter adequat del nivell de protecció que ofereix el país de destí s'avaluarà per l'Agència de Protecció de Dades atenent a totes les circumstàncies que concorrin en la transferència o categoria de transferència de dades. En particular, es tindrà en consideració la naturalesa de les dades, la finalitat i la durada del tractament o dels tractaments previstos, el país d'origen i el país de destí final, les normes de dret, generals o sectorials, vigents al país tercer de què es tracti, el contingut dels informes de la Comissió de la Unió Europea, així com les normes professionals i les mesures de seguretat en vigor en els esmentats països.»

34 LOPD estableix les següents excepcions, rellevants per a les qüestions tractades en aquest treball, al que disposa el citat article 33:

> *a*) Quan la transferència internacional de dades de caràcter personal resulti de l'aplicació de tractats o convenis en què sigui part Espanya.
>
> *b*) Quan la transferència es faci a l'efecte de prestar o sol·licitar auxili judicial internacional.
>
> *h*) Quan la transferència sigui necessària o legalment exigida per a la salvaguarda d'un interès públic. Tindrà aquesta consideració la transferència sol·licitada per una administració fiscal o duanera per al compliment de les seves competències.
>
> *k*) Quan la transferència tingui com a destí un estat membre de la Unió Europea, o un estat respecte del qual la Comissió de les Comunitats Europees, en l'exercici de les seves competències, hagi declarat que garanteix un nivell de protecció adequat.

En aquestes, en especial, la lletra *k*) i, si escau, les lletres *a*) i *b*), trobaria plena acollida allò que s'ha regulat en el Conveni Schengen i els diversos acords de cooperació judicial i policial com els EUROPOL i EURODAC; aquest últim relatiu a l'intercanvi d'empremtes dactilars respecte dels peticionaris d'asil a fi d'establir quin és el tercer país responsable en l'acceptació i tramitació de les peticions d'asilats.

5.4 Impugnació de valoracions i prova

Cal que ens detinguem un instant en el dret a les impugnacions de valoracions regulat en l'article 13 LOPD. En el treball policial les dades que obtenim davant sospitosos solen utilitzar-se per definir un perfil o per valorar el comportament d'un sospitós. A partir d'aquí, podem establir si estem davant fets que poden ser objecte d'investigació i, per tant, de l'obertura de l'oportú procediment sancionador en el cas d'infraccions administratives o del testimoni al Ministeri Fiscal o la comunicació al jutge d'Instrucció per tal d'iniciar l'oportuna instrucció penal en el cas que els fets puguin ser constitutius d'una infracció penal. Aquesta situació planteja alguna dificultat. Aquest tipus de valoracions en què s'estableixen perfils de persones a partir de les dades que se n'han obtingut —i potser les deduccions obtingudes d'un enregistrament videogràfic consisteixen en això— no sols poden ser impugnats per la persona subjecta a aquesta *valoració*, i per tant de perseguir la nul·litat de les actuacions administratives seguides amb ocasió d'aquesta valoració, sinó que, a més a més, com disposa l'apartat últim del citat article 13 LOPD, posseeix un valor probatori disminuït. Aquest apartat diu que «la valoració sobre el comportament dels ciutadans, basada en un tractament de dades, únicament podrà tenir valor probatori a petició de l'afectat». Potser convindrà donar-li a aquest precepte una interpretació restrictiva i cenyida a l'àmbit administratiu, de manera que serien les actuacions de la policia administrativa de seguretat i l'àmbit del règim sancionador administratiu on aquesta «valoracions» posseirien aquesta qualitat disminuïda; no així les derivades de l'actuació de la policia judicial.

Justament, en el marc de les actuacions com a *policia judicial*, l'enregistrament d'imatges i sons pot tenir valor probatori, però només en certes condicions.

No hi ha dubte que la captació d'imatges i sons per mitjà de videocàmeres o qualsevol altre sistema, o l'obtenció de dades personals mitjançant la intervenció de qualsevol mena de comunicació personal (sigui *analògica* —telèfon de fil, postal—, sigui *digital* —internet, sms—), a més del seu valor com a diligència d'investigació, també podrà tenir-lo com a prova preconstituïda, exactament igual que les escoltes telefòniques o les diligències en l'escorcoll d'un domicili.

Si és així, el seu règim ha de ser idèntic al de les proves preconstituïdes i sumarials respecte de les quals hi ha una rica i sòlida jurisprudència constitucional relativa al seu valor i les garanties de què ha d'estar envoltada la seva pràctica. El mitjà de captació o de comunicació no altera gens el règim constitucional de garanties de les proves preconstituïdes.

5.5 La STC 37/1998 (cas del piquet del sindicat LAB) i altres d'interès

Poques ocasions ha tingut el TC per pronunciar-se sobre aquesta matèria. Potser la mereixedora de citació és la STC 37/1998, cas del piquet del sindicat LAB. En aquesta resolució, el TC es va pronunciar sobre el cas d'una patrulla de l'Ertzaintza que, en el control que feien de l'actuació d'un piquet informatiu del sindicat LAB, va prendre fotografies i va enregistrar en vídeo les persones que formaven part del piquet.

El TC va dictar una sentència aplicant a l'actuació de l'Administració pública el que prèviament havia dit amb caràcter general per al supòsit de la instal·lació de videocàmeres i de sistemes de control i de vigilància en l'àmbit de les relacions laborals en les SSTC 98/2000, cas Casino de La Toja, i 186/2000, cas Economat d'ENSIDESA. En el primer d'aquests casos s'havien instal·lat càmeres per captar les converses dels empleats i dels clients del casino, i en el segon s'havien instal·lat uns micròfons a l'economat d'aquella indústria. El TC en ambdós casos va insistir en la proporcionalitat de les mesures. Va reconèixer que hi havia una finalitat constitucional per establir aquests sistemes de vigilància i control, però sempre que siguin proporcionats al risc que es desitja prevenir. En el cas piquet LAB, on no es va acreditar un risc cert ni per a la seguretat ni per a l'ordre públic, el TC va entendre que la mesura d'enregistrament i de control era desproporcionada i per tant lesiva del dret a la pròpia imatge dels participants en el piquet informatiu.

Les SSTC 70/2002 i 123/2002 emprenen a Espanya el denominat *comptage* en els supòsits d'intervenció de les comunicacions telefòniques (i alguna cosa es podrà importar per al cas de la conservació de les dades pels operadors de telefonia mòbil i per als proveïdors d'accés a internet). En aquests casos es plantejava la legitimitat constitucional que la policia pogués accedir sense necessitat d'una autorització judicial prèvia a les dades relatives als números de telèfon que havien trucat a l'intervingut i/o als qui aquest havia trucat, expedint tan sols un simple ofici a la companyia de telefonia corresponent. Els recurrents consideraven que l'accés a aquestes dades sense autorització judicial o consentiment dels titulars dels números de telèfon vulnerava el dret al secret de les comunicacions de l'article 18.3 CE.

L'argument que va utilitzar en ambdós casos l'advocat de l'Estat per defensar l'actuació policial i la correcció d'aquestes diligències d'investigació, que es van

emprar amb posterioritat com a proves de càrrec en les vistes orals d'ambdós processos penals, és que no afectaven el secret de les comunicacions perquè aquest només garantia el contingut de la comunicació i no les dades objectives.[16] És a dir, al seu parer, el dret al secret de les comunicacions no estendria la identitat dels intervinents en la comunicació. Per tant, segons l'advocat de l'Estat, el mer coneixement dels números de telèfon on es truca o d'on es reben trucades no afectava en absolut el secret de les comunicacions. Però, afegim ara nosaltres, sí que afecta el dret fonamental a la protecció de les dades personals. En aquest aspecte el TC no hi repara.

Cal remarcar que el TEDH, ja des del cas Malon, de 2 d'agost de 1984, ha dit que forma part de la comunicació i del seu secret no sols el contingut del que es diu sinó també la identitat dels destinataris i partícips en aquesta comunicació. Aquesta doctrina ha estat acollida de manera rotunda pel Tribunal Constitucional en les SSTC 70/2002 i 123/2002. El TC manté la mateixa posició que el TEDH i considera, per tant, que també es lesiona el dret fonamental al secret de les comunicacions si s'accedeix a aquest tipus de dades identificadores dels partícips en les comunicacions. Aquesta identitat no ha de ser necessàriament la identitat personal dels comunicants, n'hi ha prou que s'obtingui el número o el lloc des d'on es fa la trucada o l'antena que ha donat la cobertura per a la comunicació. Així doncs, subjectes aquestes dades a la garantia del secret de les comunicacions, o hi ha consentiment dels afectats per obtenir-les i utilitzar-les, o hi ha un supòsit de forma flagrant (circumstància de molt difícil concurrència en el cas d'aquestes dades i en les intervencions de comunicacions privades), o hi ha autorització judicial prèvia.

En l'únic que el TC ha estat condescendent amb l'actuació policial és que per al cas d'aquest tipus de dades no cal que l'autorització judicial tingui forma d'acte; n'hi ha prou amb la providència, sempre que contingui una succinta motivació en què s'exposin les raons per les quals s'autoritza la policia a accedir a aquest tipus d'informació.

No volem concloure aquest apartat sense cridar l'atenció sobre el fet que, fins i tot en el cas que no s'hagués incorporat en la nostra doctrina constitucional el *comptage*, el dret fonamental a la protecció de les dades personals hauria ofert tutela sobrada per a aquest tipus d'accessos.

Per l'últim, però no menys important, recordem que el TC ha matisat aquesta idea molt estesa que la captació d'imatges en llocs públics no afecta el dret fonamental a la pròpia imatge. El TC ha vingut a dir en la STC 139/2001 que, si el dret a la pròpia imatge suposa un control sobre l'ús i destí de la imatge física, el que es capti en un lloc privat o en un lloc públic tindrà rellevància a l'efecte de graduar la

16. Aquesta ha estat també la línia argumental esgrimida per la Unió Europea i el Ministeri de l'Interior espanyol per sostenir la constitucionalitat de les mesures de retenció de dades que finalment s'han fixat en la ja citada Directiva 2006/24/CE, de 15 de març de 2006, sobre la conservació de dades generades o tractades en relació amb la presentació de serveis de comunicacions electròniques d'accés públic o de xarxes públiques de comunicacions. Vegeu amb caràcter general les Conclusions de la Presidència del Consell Europeu de Brussel·les de 16 i 17 de juny de 2005 (punts 17 i següents).

proporcionalitat de la mesura de restricció, però no per determinar si s'afecta o no el dret a la pròpia imatge de la persona.

6. Consideracions finals

Deixant de banda els problemes que la LOV i el seu RV puguin plantejar des de distintes perspectives, i que han estat àmpliament subratllats pels especialistes en la matèria, l'ús d'aquestes tècniques per al desplegament de l'activitat policial, sigui en les seves funcions de *policia administrativa* o en les de *policia judicial*, comporten seriosos riscos per a la protecció de dades personals. Cal posar esment que ja hi ha tractament de dades personals, tenint en compte que les imatges i els sons ho són, i creació de fitxers, des de l'instant en què la LOV permet conservar els enregistraments durant un mes. En aquest cas, resulta ineludible tenir en compte les regles de l'article 22 LOPD.

El que és curiós, i que no pot passar inadvertit, és que, atesa la regulació de la LOV, la instal·lació de sistemes de videovigilància, fixos o mòbils, no sembla que estigui prevista per a l'exercici de les funcions pròpies de la *policia judicial*, sinó més aviat com a instrument complementari en l'exercici de les pròpies de *policia administrativa* per les FFCCSS. Justament aquí s'han centrat tots els inconvenients que fins al moment s'han posat, des de la perspectiva constitucional, a l'ús d'aquesta tècnica.

Així les coses, sembla inevitable concloure que en el cas que es desitgi utilitzar aquestes tècniques (emprar videocàmeres per enregistrar sospitosos en el marc d'una instrucció penal) o servir-se de les dades obtingudes pel seu ús (emprar els enregistraments obtinguts per les càmeres instal·lades en un edifici públic) resultarà indispensable obtenir una autorització judicial prèvia, si no el consentiment dels afectats.

Que això sigui així deriva del fet que, en primer lloc, l'ús d'aquests sistemes de videovigilància (per molt que l'apartat 1 de l'article 2 LOV pretengui negar-ho respecte d'altres drets fonamentals) suposa una restricció del dret a la protecció de dades en el cas que es conservin els enregistraments pel temps que sigui; en segon lloc, poden constituir restriccions del secret de les comunicacions, perquè l'enregistrament pot interferir una comunicació privada; i, en tercer lloc, perquè, a més a més (i insistim que malgrat el que disposa en l'article 2.1 LOV, ja que no és el legislador, ni tan sols l'orgànic, qui disposa sobre si una actuació d'un poder públic és o no limitadora i, si escau, lesiva d'un dret fonamental), és una restricció del dret de la pròpia imatge, atès que es capten imatges de persones sense comptar-ne amb el consentiment.

Voldria finalitzar la meva intervenció realitzant algunes reflexions sobre la videovigilància privada. Cal assenyalar que la utilització de sistemes de captació en el cas de la seguretat privada no té regulació. Ni la Llei ni el Reglament de Seguretat Privada (Llei 23/1992, de 30 de juliol, i Reial Decret 2364/1994, de 9 de desembre) han regulat aquesta matèria, excepte quant a les entitats bancàries, on se n'autoritza la instal·lació. No és el moment ni hi ha temps per fer una reflexió sobre aques-

ta matèria. Que quedi aquí apuntada, i que serveixi de repte perquè se sotmeti a l'estudi que requereix, sense perdre de vista que les imatges captades per aquests sistemes han demostrat una provada utilitat en la persecució de fets delictius.[17]

7. Bibliografia

Amb caràcter general cal consultar:

Guichot, E.: *Datos personales y Administración pública*, Thomson-Civitas/APDCM, Madrid, 2005.

Martínez Martínez, R.: *Una aproximación crítica a la autodeterminación informativa*, Thomson/Civitas-APDCM, Madrid, 2004.

Messía de la Cerda Ballesteros, J.A.: *La cesión o comunicación de datos de carácter personal*, Thomson-Civitas/APDCM, Madrid, 2003.

Amb caràcter específic cal consultar:

Barcelona Llop, J.: «El secreto policial. Acceso a arxivos y registros de la policía. Los ficheros automatizados de las Fuerzas y Cuerpos de Seguridad».

— «A propósito de la Ley orgánica 4/1997, de 4 de agosto, llamada de videovigilancia», *Actualidad Administrativa*, núm. 13, 1998, marginal 205.

González Urdinguio / González Gutiérrez de León: «La videovigilancia en el sistema democrático español. Análisis crítico de la Ley orgànica 4/1997, de 4 de agosto», *Revista de la Facultad de Derecho de la Universidad Complutense*, núm. 89, 1998, p. 105 i ss.

Martínez Martínez, R.: «Videovigilancia, seguridad ciudadana y derechos humanos», *Claves de la Razón Práctica*, núm. 89, 1999, p. 40 i ss.

— «Videovigilancia en lugares públicos», *Repertorio Aranzadi del Tribunal Constitucional*, núm. 17, 2000, p. 31 i ss.

Magrot Servet, V.: «Consideraciones sobre la nueva Ley que regula la utilización de las videocámeras por las Fuerzas y Cuerpos de Seguridad del Estado», *Revista del Poder Judicial*, núm. 47, 1997, p. 277 i ss.

Padrós Reig, C.: «Videovigilancia y Estado autonómico. Comentario a propósito de la actividad normativa de despliegue de la Ley orgànica 4/1997», *Revista de Administración Pública*, núm. 151, 2000, p. 465 i ss.

Ull Salcedo, M.V.: «El derecho a la intimidad como límite a la videovigilancia», *Revista de Derecho Político*, núm. 63, 2005, p. 177 i ss.

17. Vegeu el cas de la STC 206/2003 sobre l'ús com a prova de les cintes amb imatges captades per una càmera instal·lada al lloc en què hi havia un caixer automàtic d'una entitat bancària.