Generalitat de Catalunya
Escola d'Administració Pública de Catalunya

apdcat Agència Catalana de Protecció de Dades

El dret a la protecció de dades de caràcter personal

Autors

- Agència catalana de protecció de dades (autoria dels continguts): Joana Marí, Carles San José, Ramon M. Miralles i Jordi Ferreres.
- Fotografies incloses al curs: Laura Trilla.
- Dibuix: Xavier Belanche
- Escola d'Administració Pública de Catalunya (coordinació tècnica i pedagògica): Eva Gea.

Llicència

Darrera actualització: Juny 2010

Índex de continguts

Unitat 1: Introducció. Com neix el dret a la protecció de dades

El dret a l'autodeterminació informativa

L'**article 18 de la Constitució espanyola** (d'ara endavant, CE) regula el dret a l'honor, la intimitat personal i familiar i el dret a la pròpia imatge. Aquests drets s'han definit com a drets de llibertat emmarcats dins dels drets de la personalitat, és a dir, drets que protegeixen aspectes de les persones directament relacionats amb la seva condició d'ésser humà. El Tribunal Constitucional (d'ara endavant, TC) ha definit el dret a la intimitat de l'article 18 CE com:

"(…) *una derivación de la dignidad de la persona que implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana*" (STC 209/1988, sentència de 10 de novembre de 1988. FJ 3).

És a dir, és la **facultat de l'individu d'evitar ingerències en àmbits especialment reservats de la vida de la persona** (per exemple, el domicili familiar, la correspondència…).

D'altra banda, l'article 18.4 de la CE estableix que:

"*La llei limitarà l'ús de la informàtica per garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets*".

Aquest reconeixement dóna entrada a un fenomen que ara ja no podem considerar nou, però sí relativament poc conegut, i que ha comportat un canvi d'estructura a la nostra societat. L'aparició

de la informàtica i la seva combinació amb les telecomunicacions ha conduït a l'anomenada "societat de la informació". La informació ha esdevingut un dels motors de la nostra societat (un actiu per a les empreses i administracions públiques). La informació s'ha convertit en un bé de gran valor i ha deixat de servir només per a un fi concret, en un moment concret, ja que han desaparegut conceptes com temps i espai. També ha desaparegut el concepte d'oblit de la informació. És interessant com una afirmació de l'any 1978 continua sent vigent ara (i potser amb major sentit):

"*Las posibilidades de aplicación de la tecnología, […], constituyen las manifestaciones de un mundo en el cual la humanidad está desarrollando una nueva fisonomía espiritual, tanto que la mentalidad tecnológica se presenta como una segunda y renovada naturaleza suya*" (FROSINI, V., *Cibernética, derecho y sociedad*, Colección Ciencias Jurídicas, Editorial Tecnos, Madrid, 1982, pág. 59).

Aquesta "*fisonomía espiritual*" de la humanitat ha generat l'aparició d'un nou dret, el **dret a l'autodeterminació informativa o dret a la protecció de dades personals**. Aquest dret, que va néixer lligat al dret a la intimitat, s'ha convertit en un dret per ell mateix ateses les noves necessitats de protecció de l'individu davant dels nous riscos que poden sorgir d'un mal ús de les tecnologies de la informació i la comunicació.

Tot i que l'aparició d'aquest dret no ha seguit l'*iter natural* dels drets clàssics (rebuig de la societat a una realitat que mitjançant la pressió social es converteix en valors polítics que finalment passen a l'ordenament jurídic), ara, a la nostra societat comença a existir una consciència social pel que fa a l'existència d'un dret a la protecció de dades. Han estat els experts de les noves tecnologies, juristes i filòsofs, els que davant el coneixement de les possibilitats que generen aquestes van començar a parlar d'aquest nou dret.

En l'actualitat, davant situacions molt concretes es comença a generar aquesta consciència social. Un exemple d'això seria la videovigilància.

Les dades es van recollint, fins i tot abans del nostre naixement (dades mèdiques) i continuen acumulant-se al llarg de tota la nostra vida. En cadascuna de les fases del nostre desenvolupament com a persones (escola, universitat, feina, salut, aficions, lectures, compres, crèdits) es van recollint dades que amb les eines oportunes poden permetre un coneixement de nosaltres fins i tot millor del que faríem nosaltres mateixos. Davant això, la informació es converteix en una nova forma de poder per a aquella persona que la pot recollir i tractar.

El dret a la protecció de dades personals neix, doncs, com una eina per protegir-nos davant d'aquesta nova realitat. No obstant això, no podem oblidar que no hi ha drets absoluts i, per tant, hi haurà altres drets i béns que també hauran de ser protegits.

Caldrà, per tant, delimitar quina és la configuració d'aquest dret per poder realitzar una correcta ponderació en situacions de conflicte.

Configuració del dret a la protecció de dades personals

Què protegeix el dret a la protecció de dades?

Amb la creació, el manteniment i la interconnexió de bases de dades es pot incidir de manera molt important en qualsevol dels aspectes de la vida d'una persona. El dret a la protecció de dades personals vol garantir el control de l'individu sobre el conjunt d'informacions que fan referència a la seva vida. Des de la perspectiva del dret a la protecció de dades, no hi ha dades sense interès: totes les dades personals queden protegides per aquest dret, el qual només podrà ser

correctament garantit si l'individu pot controlar la utilització de totes i cadascuna de les dades que fan referència a la seva vida, amb independència del nivell d'ingerència que ens puguin semblar que tenen en la seva vida privada.

"*El grado de sensibilidad de las informaciones ya no depende únicamente de si afectan o no a procesos de la intimidad. Hace falta conocer la relación de utilización de un dato para poder determinar sus implicaciones para el derecho de la personalidad*"(Sentència del Tribunal Constitucional alemany, de 15 de desembre de 1983, sobre la Llei del cens de 1983. *Boletín de Jurisprudencia Constitucional*, núm. 33, 1984, pág. 154).

El dret a la protecció de dades és un dret de la personalitat, per tant, directament vinculat amb la dignitat de la persona, la llibertat personal i el lliure desenvolupament de la personalitat.

Els conceptes de dignitat i llibertat van necessàriament units. Estan encaminats a possibilitar que la persona pugui decidir de forma autònoma i independent, és a dir, amb llibertat, sobre les accions que vol realitzar. És en la lliure decisió de les accions que duem a terme com anem desenvolupant la nostra personalitat.

La llibertat i el lliure desenvolupament de la personalitat, que són el camí cap al respecte de la dignitat humana, configuren la base del bé jurídic protegit a l'article 18.4 de la CE. Aquella persona que se senti insegura per no poder conèixer qui sap coses de la seva vida o què és el que sap no podrà actuar lliurement, és a dir, no podrà optar lliurement respecte d'allò que vol ser i es convertirà en allò que es dedueixi, s'interpreti o es generi a partir de la interconnexió de dades relatives a la seva vida. Per evitar-ho, s'han d'establir les garanties necessàries perquè l'individu pugui controlar la seva vida, per poder controlar totes aquelles informacions que surten del seu entorn.

El mateix Tribunal Constitucional ja va reconèixer aquest dret l'any 1993, en el cas Olaverri, tot i que en aquest primer moment no parla de dret a la protecció de dades, sinó de llibertat informàtica:

> *"[…] nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma que en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos […]"(STC 254/1993, de 20 de juny. Recurs d'empara núm. 1827/1990. BOE de 18 d'agost de 1993. FJ 4).*

El Tribunal Constiucional defineix aquest dret des d'una doble perspectiva:

- com a dret autònom
- com a institut de garantia de la resta de drets i llibertats.

Tot i que en aquesta primera jurisprudència només es reconeix tímidament l'existència d'aquest nou dret, posteriorment, l'any 1998, en el cas Renfe, el fonament cinquè d'aquesta sentència indica:

> *"[…] ha de concluirse que tuvo lugar una lesión del art. 28.1 CE en conexión con el art.18.4 CE. Este no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, […], sino que además,* ***consagra un derecho fundamental autónomo*** *a controlar el flujo de informaciones que conciernen a cada persona –a la privacidad según la expresión utilizada en la Exposición de motivos de la LORTAD- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos […]"*

(STC 11/1998, sentència de 13 de gener de 1998. Recurs d'empara núm. 2264/1996. BOE de 12 de febrer de 1998).

D'altra banda, no podem oblidar que els tractats internacionals també ens serveixen per delimitar els drets i, concretament, respecte del dret a la protecció de dades hem de tenir presents els següents textos:

- Conveni 108/1981 del Consell d'Europa, per a la protecció de les persones en relació amb al tractament automatitzat de dades de caràcter personal. L'article primer estableix que té per finalitat garantir el dret a la vida privada respecte del tractament de dades personals de tota persona física, amb independència de la seva nacionalitat o residència.
- Conveni per a la protecció dels drets humans i de les llibertats fonamentals. L'article 8.1 reconeix el dret a la vida privada i familiar. El Tribunal Europeu de Drets Humans, aplicant aquest article, ha reconegut el dret a la protecció de dades personals.
- Declaració Universal dels Drets Humans. L'article 12 reconeix el dret a la vida privada.
- Pacte Internacional de Drets Civils i Polítics. Reconeix també, a l'article 17, el dret a la vida privada i prohibeix les ingerències arbitràries.

A partir de totes aquestes referències podem determinar quin és el contingut mínim del dret a la protecció de dades personals, és a dir, aquell contingut sense el qual perd la seva virtualitat. Les restriccions a aquest contingut només podran derivar-se de la Constitució. En definitiva, es vol protegir la lliure determinació de la persona respecte del conjunt de dades que es refereixen a ella. Aquesta possibilitat d'actuar lliurement en darrer terme protegeix el principi democràtic. L'individu que controla les seves dades pot actuar més lliurement, no només respecte de la seva vida privada, sinó que també pot participar de forma més lliure en la vida social, política i econòmica de la comunitat de què forma part.

Per assolir aquest objectiu cal que la persona tingui determinades facultats d'actuació que li permetin controlar les seves dades.

De la Constitució espanyola, interpretada conforme als tractats i convenis internacionals (per tant, sense anar a una norma que desenvolupi aquesta qüestió) ja en podem extreure aquestes facultats que permetran determinar qui utilitza les meves dades, per a què, quant de temps, etc. Per tant, sembla que el principi que ha de regir aquest dret és el del consentiment conscient i informat de les circumstàncies rellevants de la utilització de les dades, i que una de les primeres facultats que l'han d'integrar és la d'informació respecte d'aquelles circumstàncies necessàries per controlar les dades que ens demanen.

Un cop recollides les dades, hem de poder continuar controlant-les:

- verificar l'ús que se n'està fent;
- corregir les dades amb el pas del temps;
- tenir la possibilitat de demanar que deixin de ser utilitzades.

Així apareixen les facultats d'accés, de rectificació i cancel·lació de les dades personals.

En definitiva, el contingut del dret a la protecció de dades personals ve configurat per la protecció de la vida privada mitjançant el control de la utilització de les dades personals pròpies, hi ha de regir el principi general del consentiment i s'hi han de garantir les facultats d'informació en el moment de la recollida de les dades, d'accés a les dades tractades per conèixer el contingut exacte del fitxer, de rectificació de les dades incorrectes i de cancel·lació d'aquelles dades que per alguna circumstància no hagin de ser tractades.

A qui protegeix el dret a la protecció de dades personals?

Tot i que l'article 18.4 de la CE ens parla de "ciutadans", no podem pensar que el dret només protegeix els ciutadans espanyols. Hem de tenir en compte, d'una banda, la necessitat

d'interpretació conjunta de la Constitució i dels tractats i convenis internacionals on es reconeix el dret a tota persona física i, de l'altra, que tal com hem vist, estem davant d'un dret de la personalitat directament vinculat a la dignitat humana i, per tant, que es reconeix a totes les persones atesa la seva condició. En conseqüència, el dret a la protecció de dades es reconeix a totes les persones físiques amb independència de la seva nacionalitat.

Quins límits té el dret a la protecció de dades personals?

Un límit a un dret fonamental és qualsevol restricció a la seva eficàcia i, en tot cas, ha de respectar el marc constitucional.

Els límits han de ser interpretats d'acord amb el principis següents:

1. Interpretació sistemàtica de la Constitució.
2. Interpretació a favor de la major efectivitat dels drets.
3. Els poders públics estan obligats a adoptar totes les mesures necessàries per assolir la plena efectivitat dels drets.
4. L'establiment de límits als drets ha d'estar sempre justificat.
5. Proporcionalitat, és a dir, el resultat de la mesura limitativa ha de comportar més avantatges per a l'interès general que perjudicis respecte dels béns o valors limitats.

Tots els drets tenen límits, no n'hi ha cap d'absolut, però els límits han d'estar constitucionalment justificats. Així, l'article 53.1 de la CE estableix que el legislador pot limitar l'exercici dels drets sempre que en respecti el contingut essencial.

A banda dels límits que es deriven del conflicte amb altres drets i llibertats, també podem trobar determinats béns jurídics constitucionalment protegits que poden entrar en conflicte amb el dret a la protecció de dades personals, com per exemple els següents:

- defensa de l'Estat
- sosteniment de la despesa pública
- principis rectors de l'ordenament jurídic
- protecció de drets i llibertats dels ciutadans i garantia de la seguretat ciutadana per part de les forces i cossos de seguretat de l'Estat.

Al llarg d'aquest curs analitzarem com es dota de contingut i eficàcia el dret a la protecció de dades personals a partir del seu desenvolupament normatiu. Tot i això, no podem oblidar que el dret a la protecció de dades es pot exercir sense que existeixi una llei que el desenvolupi.

Unitat 2: Desenvolupament normatiu del dret a la protecció de dades

Marc normatiu

Com hem vist en el primer mòdul, el dret a la protecció de dades personals és un dret fonamental que deriva de l'article 18.4 de la CE, i si ens fixem en el primer cas que arriba al Tribunal Constitucional relatiu a la defensa d'aquest dret, el cas Olaverri, el Tribunal reconeix a la persona demandant el dret a accedir als fitxers automatitzats que sobre ell tenia una administració pública, sense que existís una llei que desenvolupés aquest dret, és a dir, aplicant directament l'article 18.4 de la CE. Així veiem que aquest és un dret dels que s'anomenen d'exercici directe i, per tant, que no requereix d'una normativa de desenvolupament per poder ser exercit i defensat davant dels tribunals.

En tot cas, atès que ens trobem davant d'un dret fonamental, la regulació del seu contingut s'havia de portar a terme mitjançant una llei orgànica i, en aquest cas, la Llei orgànica 5/1992, de 29 d'octubre, de regulació del tractament automatitzat de dades de caràcter personal (en endavant, LORTAD), ha estat la primera norma a Espanya que ha regulat el dret a la protecció de dades personals.

Concretament, la LORTAD el que protegeix és exclusivament el tractament automatitzat de les dades personals (pensem que l'article 18.4 de la CE indica que el legislador ha de garantir els drets i les llibertats establint límits a l'ús de la informàtica).

De fet, al preàmbul, la LORTAD ja indica que:

“La ley está animada por la idea de implantar mecanismos cautelares que prevengan las violaciones de la privacidad que pudieran resultar del tratamiento de la información”.

L'any 1995 s'aprova la Directiva 95/46/CE, del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (en endavant, Directiva 95/46/CE) la qual, en l'article 1.1, estableix com a objecte:

> *"Els Estats membres garanteixen, d'acord amb les disposicions d'aquesta Directiva, la protecció de les llibertats i dels drets fonamentals de les persones físiques i, en particular, del dret a la intimitat pel que fa al tractament de les dades personals"*

Aquesta directiva va ser adaptada en l'ordenament jurídic espanyol a través de la Llei orgànica 15/1999, de protecció de dades de caràcter personal (en endavant, LOPD), que deroga la

LORTAD i que estableix els principis i les garanties del dret a la protecció de dades personals, concretats en una sèrie d'obligacions per a aquelles persones i entitats, públiques i privades, que tracten dades personals. Una de les principals novetats de la LOPD és que ja no només es protegeixen els tractaments automatitzats de dades personals, sinó també els tractaments no automatitzats o manuals de dades personals.

Aquesta llei ha estat desenvolupada pel Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la LOPD.

D'altra banda, a Catalunya s'ha creat una autoritat de control específica per a la garantia del dret a la protecció de dades, l'Agència Catalana de Protecció de Dades, que neix amb la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades.

Finalment, cal indicar que el mateix Estatut d'Autonomia de Catalunya reconeix, a l'article 31, el dret a la protecció de les dades personals.

Trobareu enllaços a normativa d'interès al *bloc de* **Normativa** d'aquest curs d'Aula Virtual.

Definicions

L'estudi de la protecció de dades exigeix conèixer una sèrie de conceptes que són específics d'aquesta matèria i que seran utilitzats al llarg de tot el curs.

Tant la Directiva 95/46/CE, com la LOPD recullen un llistat de definicions, però ha estat el RLOPD el text que les ha concretat de manera més detallada, per tant utilitzarem les definicions que aquesta norma recull a l'article 5 per començar a estudiar la normativa de protecció de dades.

Per tal de tenir identificats i agrupats el conceptes que s'utilitzaran al llarg del curs, a continuació es recullen les definicions que inclou el nou RLOPD, però agrupades d'acord amb el que podem anomerar el cicle de vida de les dades (recollida, tractament, comunicació i conservació). No s'entra, aquí, en l'explicació detallada de cada concepte, atès que això es farà dins de les diferents unitats que configuren el curs.

- **Dades de caràcter personal**: qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus que concerneix persones físiques identificades o identificables.
- **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 aquesta identificació requereix terminis o activitats desproporcionats.
- **Procediment de dissociació**: qualsevol tractament de dades personals que permeti l'obtenció de dades dissociades.
- **Dada dissociada**: la que no permet identificar una persona afectada o interessada.
- **Dades de caràcter personal relacionades amb la salut**: informacions que concerneixen la salut passada, present i futura, física o mental, d'un individu. En particular, es consideren dades relacionades amb la salut de les persones les referides al seu percentatge de discapacitat i a la seva informació genètica.
- **Persona afectada o interessada**: persona física titular de les dades que siguin objecte del tractament.
- **Consentiment de la persona interessada**: qualsevol manifestació de voluntat lliure, inequívoca, específica i informada, mitjançant la qual la persona interessada consent el tractament de dades personals que la concerneixen.

- **Fitxer**: qualsevol conjunt organitzat de dades de caràcter personal que permeti l'accés a les dades d'acord amb uns criteris determinats, sigui quina sigui la forma o modalitat de la creació, l'emmagatzematge, l'organització i l'accés.
- **Fitxer no automatitzat**: qualsevol conjunt de dades de caràcter personal organitzat de forma no automatitzada i estructurat d'acord amb criteris específics relatius a persones físiques, que permeti accedir sense esforços desproporcionats a les seves dades personals, tant si aquell és centralitzat, descentralitzat o repartit de forma funcional o geogràfica.
- **Fitxers de titularitat privada**: fitxers els responsables dels quals són les persones, empreses o entitats de dret privat, independentment de qui tingui la titularitat del seu capital o de la procedència dels seus recursos econòmics, així com els fitxers els responsables dels quals són les corporacions de dret públic, si és que aquests fitxers no estan estrictament vinculats a l'exercici de potestats de dret públic que els atribueix la seva normativa específica.
- **Fitxers de titularitat pública**: fitxers els responsables dels quals són els òrgans constitucionals o amb rellevància constitucional de l'Estat o les institucions autonòmiques amb funcions anàlogues a aquests òrgans, les administracions públiques territorials, així com les entitats o organismes que hi estan vinculats o en depenen i les corporacions de dret públic, sempre que la seva finalitat sigui l'exercici de potestats de dret públic.
- **Tractament de dades**: qualsevol operació o procediment tècnic, ja sigui automatitzat o no, que permeti la recollida, l'enregistrament, la conservació, l'elaboració, la modificació, la consulta, la utilització, la cancel·lació, el bloqueig o la supressió de dades, així com les cessions de dades que resultin de comunicacions, consultes, interconnexions i transferències.
- **Responsable del fitxer o del tractament**: persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu que sol o conjuntament amb altres decideixi sobre la finalitat, el contingut i l'ús del tractament, encara que no ho faci materialment.

També poden ser responsables del fitxer o del tractament els ens sense personalitat jurídica que actuïn en el tràfic com a subjectes diferenciats.

- **Encarregat del tractament**: persona física o jurídica, pública o privada, o òrgan administratiu que sol o conjuntament amb altres tracta dades personals per compte del responsable del tractament o del responsable del fitxer, com a conseqüència de l'existència d'una relació jurídica que l'hi vincula i delimita l'àmbit de la seva actuació per a la prestació d'un servei.

També poden ser encarregats del tractament els ens sense personalitat jurídica que actuïn en el tràfic com a subjectes diferenciats.

- **Cessió o comunicació de dades**: tractament de dades que implica revelar-les a una persona diferent de la persona interessada.
- **Destinatari o cessionari**: persona física o jurídica, pública o privada, o òrgan administratiu a qui es revelin les dades.

També poden ser destinataris els ens sense personalitat jurídica que actuïn en el tràfic com a subjectes diferenciats.

- **Tercer**: persona física o jurídica, pública o privada, o òrgan administratiu diferent de la persona afectada o interessada, del responsable del tractament, del responsable del fitxer, de l'encarregat del tractament i de les persones autoritzades per tractar les dades sota l'autoritat directa del responsable del tractament o de l'encarregat del tractament.

També poden ser tercers els ens sense personalitat jurídica que actuïn en el tràfic com a subjectes diferenciats.

- **Transferència internacional de dades**: tractament de dades que suposa una transmissió d'aquestes dades fora del territori de l'Espai Econòmic Europeu, tant si constitueix una cessió o comunicació de dades, com si té per objecte la realització d'un tractament de dades per compte del responsable del fitxer establert en el territori espanyol.

- **Exportador de dades personals**: persona física o jurídica, pública o privada, o òrgan administratiu situat en el territori espanyol que faci, d'acord amb el que disposa aquest Reglament, una transferència de dades de caràcter personal a un tercer país.
- **Importador de dades personals**: persona física o jurídica, pública o privada, o òrgan administratiu receptor de les dades en cas de transferència internacional d'aquestes dades a un tercer país, tant si és la persona responsable del tractament, l'encarregada del tractament o una tercera persona.
- **Cancel·lació**: procediment en virtut del qual la persona responsable cessa en l'ús de les dades. La cancel·lació implica el bloqueig de les dades, consistent en la identificació i la reserva d'aquestes amb la finalitat d'impedir-ne el tractament excepte per posar-les a disposició de les administracions públiques, jutges i tribunals, per atendre les possibles responsabilitats nascudes del tractament i només durant el termini de prescripció de les responsabilitats esmentades. Una vegada transcorregut aquest termini, s'han de suprimir les dades.

L'article 5 del RLOPD també recull les definicions corresponents als termes utilitzats a l'hora de tractar les mesures de seguretat tècniques i organitzatives. Aquestes definicions es veuran en la unitat corresponent a l'estudi de la seguretat dels fitxers i tractaments que contenen dades personals.

L'article 3 de la LOPD també defineix què s'entén per fonts accessibles al públic, i això es concreta a l'article 7 del RLOPD, segons el qual tenen el caràcter de fonts accessibles al públic:

- El cens promocional
- Les guies de serveis de comunicacions electròniques, en els termes que preveu la normativa específica.
- Les llistes de persones pertanyents a grups de professionals que continguin únicament les dades del nom, el títol, la professió, l'activitat, el grau acadèmic, l'adreça professional i la indicació de la seva pertinença al grup. L'adreça professional pot incloure les dades del domicili postal complet, el número telefònic, el número de fax i l'adreça electrònica. En el cas dels col·legis professionals, es poden indicar com a dades de pertinença al grup les de número de col·legiat, data d'incorporació i situació d'exercici professional.
- Els diaris i butlletins oficials.
- Els mitjans de comunicació social.

Però, per ser fonts accessibles al públic cal que la seva consulta la pugui fer qualsevol persona no impedida per una norma limitativa, o sense més exigència que, si escau, l'abonament d'una contraprestació.

Àmbit d'aplicació

L'article 2 de la LOPD regula l'àmbit d'aplicació d'aquesta norma, tant respecte de l'àmbit material com del territorial. Així mateix, s'hi estableixen aquelles matèries que, o bé en queden excloses, o bé només es regeixen parcialment per la LOPD.

Àmbit material

La LOPD s'aplica a les dades de caràcter personal enregistrades en un suport físic que les fa susceptibles de tractament, i a qualsevol modalitat d'ús posterior d'aquestes dades fet pels sectors públic i privat.

Cal recordar que l'objecte de la normativa de protecció de dades és garantir i protegir el conjunt de drets fonamentals i llibertats públiques de les persones físiques en els tractaments de dades personals, tant si aquests tractaments es duen a terme de forma automatitzada o manual.

Per tant, en el moment de determinar si és d'aplicació la LOPD hem de tenir en compte els conceptes següents: persona física, dada de caràcter personal, tractament i suport físic.

Per tal de delimitar el concepte de dada de caràcter personal, és interessant el relatiu al concepte de dada de caràcter personal del Grup de treball de l'article 29.

Àmbit territorial

L'article 2.1 de la LOPD regula el principi de territorialitat, és a dir, determina l'abast geogràfic d'aplicació de la norma. Hi trobem dos aspectes claus: el lloc de realització del tractament i la ubicació del responsable del tractament.

Aquesta delimitació és important si tenim present que les noves tecnologies comporten grans possibilitats de tractament i que el lloc on es realitzi aquest tractament és indiferent, cosa que podria comportar, si no s'adoptessin les garanties adequades, que es buidés de contingut el dret a la protecció de dades personals.

Així, l'article 2.1 de la LOPD estableix que la llei serà d'aplicació quan:

- el tractament s'efectuï en territori espanyol, en el marc de les activitats d'un establiment del responsable del tractament.
- al responsable del tractament no establert en territori espanyol li sigui aplicable la legislació espanyola, d'acord amb les normes de dret internacional públic.
- el responsable del tractament no estigui establert en el territori de la Unió Europea i utilitzi, en el tractament de dades, mitjans situats en territori espanyol, llevat que aquests mitjans s'utilitzin únicament amb finalitats de trànsit.

Matèries excloses de l'àmbit d'aplicació

Pel que fa a aquest punt, la LOPD regula aquells supòsits en què les garanties establertes per a les dades personals no són d'aplicació, ateses les característiques del tractament.

Així, l'article 2.2 de la LOPD indica que aquesta llei no és aplicable:

- als fitxers mantinguts per persones físiques en l'exercici d'activitats exclusivament personals o domèstiques. Aquesta excepció ha de ser interpretada de forma estricta ("exclusivament"). Per tant, si tenim una agenda i la utilitzem amb fins personals i professionals, aquesta última finalitat fa que entri dins del marc d'aplicació de la LOPD.

El RLOPD, a l'article 4.a), indica que: "Només es consideren relacionats amb activitats personals o domèstiques els tractaments relatius a les activitats que s'inscriuen en el marc de la vida privada o familiar dels particulars."

- als fitxers sotmesos a la normativa sobre protecció de matèries classificades.

La Llei 9/1968, de 5 d'abril, de secrets oficials, modificada per la Llei 48/1978, de 7 d'octubre, estableix que poden ser declarades matèries classificades els assumptes, els actes, els documents, les informacions, les dades i els objectes el coneixement dels quals, per persones no autoritzades, pugui danyar o posar en risc la seguretat i la defensa de l'Estat.

- als fitxers establerts per a la investigació del terrorisme i de formes greus de delinqüència organitzada. No obstant això, en aquests supòsits, el responsable del fitxer ha de comunicar-ne prèviament l'existència, les característiques generals i la finalitat a l'Agència de Protecció de Dades.

Matèries parcialment excloses

En els supòsits que s'esmenten a continuació, les matèries enunciades es regeixen per la normativa sectorial concreta que les regula i la LOPD només s'aplica en allò previst específicament per a aquestes matèries.

- Els fitxers regulats per la legislació de règim electoral. En aquest cas, hem de tenir en compte la legislació que regula el cens electoral i els padrons municipals.
- Els fitxers que tinguin finalitats exclusivament estadístiques i estiguin emparats per la legislació estatal o autonòmica sobre la funció estadística pública. Hem de tenir present que en aquest àmbit s'ha de fer una interpretació restrictiva ("exclusivament"). El mateix RLOPD ens indica, a l'article 9.1, que no es considera incompatible el **tractament de les dades de caràcter personal amb fins** històrics, **estadístics** o científics i que per tal de determinar **aquests fins**, cal atenir-se a la legislació que en cada cas sigui aplicable i, en particular, **al que disposen la Llei 12/1989, de 9 de maig, reguladora de la funció estadística pública** i les disposicions que la despleguen, així com a la normativa autonòmica referent a aquestes matèries.

A Catalunya hem de tenir present el que regula la Llei 23/1998, de 30 de desembre, d'estadística de Catalunya.

- Els fitxers que tinguin com a objecte l'emmagatzematge de les dades contingudes en els informes personals de qualificació a què es refereix la legislació del règim del personal de les Forces Armades.

En aquest àmbit trobem la Llei 17/1999, de 18 de maig, que regula el règim del personal de les Forces Armades.

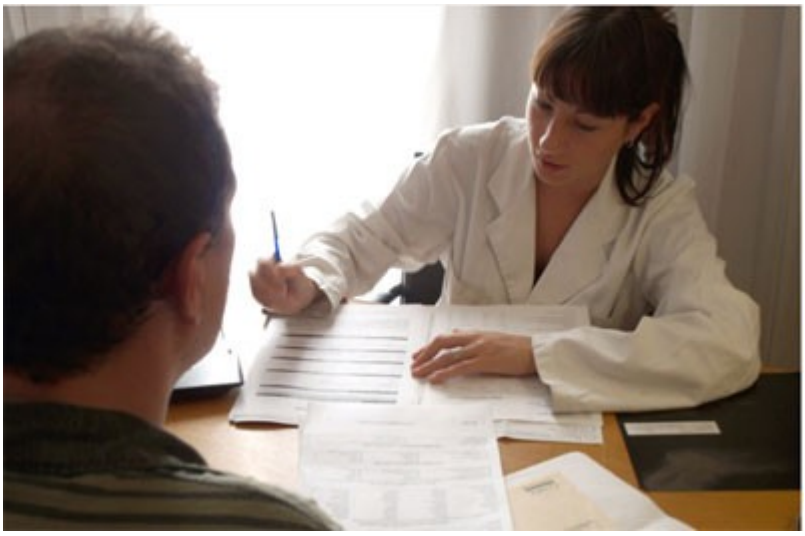
- Els fitxers derivats del Registre Civil i del Registre Central de Penats i Rebels. En aquests casos cal atenir-se a la regulació establerta, entre d'altres, a la Llei de 8 de juny de 1957, reguladora del Registre Civil, i a la Llei orgànica 1/1979, de 26 de setembre, general penitenciària.
- Els fitxers procedents d'imatges i sons obtinguts mitjançant la utilització de videocàmeres per les forces i els cossos de seguretat, d'acord amb la legislació sobre la matèria. En aquest cas, cal anar a la Llei orgànica 4/1997, de 4 d'agost, sobre la utilització de videocàmeres per les forces i els cossos de seguretat i les normes que la desenvolupen.

Finalment, cal recordar el que regula l'article 2 del RLOPD, en què s'estableixen certs àmbits exclosos de la normativa de protecció de dades que poden generar problemes d'aplicabilitat o d'interpretació:

- article 2.2 del RLOPD: Aquest Reglament no és aplicable als tractaments de dades referides a persones jurídiques, ni als fitxers que es limitin a incorporar les dades de les persones físiques que hi prestin els seus serveis, consistents únicament en el nom i els cognoms, les funcions o els llocs exercits, així com l'adreça postal o electrònica, el telèfon i el número de fax professionals.
- article 2.3 del RLOPD: Així mateix, les dades relatives a empresaris individuals, quan hi facin referència en la seva qualitat de comerciants, industrials o naviliers, també s'han d'entendre excloses del règim d'aplicació de la protecció de dades de caràcter personal.
- article 2.4 del RLOPD: Aquest Reglament no és aplicable a les dades referides a persones mortes. No obstant això, les persones vinculades al mort, per raons familiars o anàlogues, es poden dirigir als responsables dels fitxers o tractaments que continguin dades de la persona morta amb la finalitat de notificar l'òbit, aportant l'acreditació suficient, i sol·licitar, quan escaigui, la cancel·lació de les dades.

Aquests casos, principalment els apartats 2 i 3 d'aquest article, han generat dificultats d'interpretació pel que fa a les situacions en què són d'aplicació. En tot cas, hem de tenir en compte que ens trobem davant d'un dret fonamental i que, per tant, qualsevol límit s'ha d'interpretar de manera restrictiva.

Unitat 3: Principis i obligacions del tractament de dades personals



Qualitat de les dades

El tractament de dades personals en qualsevol de les seves fases (recollida, elaboració, cessió, emmagatzematge…) ha de complir una sèrie de principis relatius a la qualitat de les dades que s'hi tracten.

L'article 4 de la LOPD estableix aquests principis:

Principi de proporcionalitat

Només es poden recollir aquelles dades que siguin adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats per als quals s'han obtingut. És a dir, només es poden recollir i tractar les dades personals estrictament necessàries per a la finalitat de què es tracti.

Principi de finalitat

Les dades s'han de recollir per a finalitats determinades, explícites i legítimes. Les dades no poden ser utilitzades per a finalitats incompatibles a les que varen motivar la seva recollida.

El concepte finalitats "incompatibles" ha generat importants problemes d'interpretació i aplicació pràctica, i la doctrina i la jurisprudència entenen que l'ús d'aquest terme ha estat degut a una traducció poc precisa de l'article 6 de la Directiva 95/46/CE. Aquest concepte s'ha d'interpretar de manera molt restrictiva i fent una interpretació sistemàtica de tota la LOPD. No es considera incompatible el tractament de les dades de caràcter personal amb fins històrics, estadístics o científics.

Quan les dades ja no siguin necessàries per a la finalitat que ha motivat la seva recollida, el responsable del fitxer ha de cancel·lar-les.

No hem de confondre aquesta obligació del responsable del fitxer amb el dret de cancel·lació de la persona interessada.

En tot cas, les dades es poden conservar durant els terminis en què es pugin exigir responsabilitats derivades de la relació jurídica existent.

Principi d'exactitud

Les dades s'han de mantenir actualitzades i han de respondre a la situació actual de la persona interessada. Si les dades són errònies, han de ser cancel·lades i substituïdes per les correctes en el termini de 10 dies des que es coneix la inexactitud.

No hem de confondre aquesta obligació del responsable del fitxer amb el dret de rectificació de la persona interessada.

El RLOPD indica que es consideren exactes les dades que han estat recollides directament de la persona interessada.

En els supòsits en els quals les dades rectificades o cancel·lades hagin estat objecte de cessió (i es conegui a qui s'han cedit) caldrà comunicar, dins del termini de 10 dies, a les persones o entitats a qui han estat cedides, que s'ha realitzat aquesta rectificació o cancel·lació. Aquests últims, en el termini de 10 dies des de la recepció de la notificació, han de procedir a rectificar o cancel·lar les dades que ells tractin.

Principi de conservació

Les dades han de ser emmagatzemades de manera que es permeti l'exercici del dret d'accés, excepte si han estat cancel·lades. Les dades es poden conservar durant un termini superior al necessari per assolir les finalitats que van motivar la seva recollida, sempre que no sigui possible identificar la persona interessada, és a dir: s'han de fer anònimes.

Principi de lleialtat i licitud

La LOPD prohibeix la recollida de dades per mitjans fraudulents, deslleials o il·lícits i el RLOPD indica que les dades han de ser tractades de manera lleial i lícita.

Deure del secret

La LOPD estableix que totes aquelles persones que intervenen en qualsevol fase del tractament de les dades personals estan obligades al secret professional, pel que fa a les dades, i al deure de guardar-les. Aquestes obligacions subsisteixen fins i tot després de finalitzar les seves relacions amb el responsable o titular del fitxer o amb l'encarregat del tractament.

És important que el responsable del fitxer i l'encarregat del tractament informin a totes aquelles persones que intervenen en el tractament de dades personals sobre quines són les seves obligacions respecte de la normativa de protecció de dades personals.

Dret d'informació

El dret d'informació en el moment de la recollida de les dades és el punt de partida de la legitimitat de tot el tractament de les dades. S'ha de tenir present que el dret a la protecció de dades personals comporta la possibilitat de control de les dades personals per part de la persona que

n'és titular i, per tant, aquest dret només es podrà fer efectiu si es coneixen les circumstàncies principals del tractament que es porta a terme.

Dades recollides de la persona interessada

Aquest dret està regulat a l'article 5.1 de la LOPD, en què s'estableix que les persones interessades a les quals se sol·licitin dades personals han de ser prèviament informades de manera expressa, precisa i inequívoca:

a) de l'existència d'un fitxer o un tractament de dades de caràcter personal, de la finalitat de la recollida de les dades i dels destinataris de la informació.

b) del caràcter obligatori o facultatiu de la resposta a les preguntes que els siguin plantejades.

c) de les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.

d) de la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.

e) de la identitat i l'adreça del responsable del tractament o, si s'escau, del seu representant.

Aquestes són les anomenades clàusules informatives. És important tenir en compte que, amb independència de quin sigui el procediment de recollida de les dades (formularis, telèfon, internet…) s'ha de facilitar el dret d'informació. En tot cas, si les dades es recullen mitjançant qüestionaris o impresos ha de constar-hi clarament llegible la informació relativa al tractament de les dades que es vol portar a terme (article 5.2 de la LOPD).

Tan important com el contingut de la clàusula informativa és que aquesta clàusula estigui redactada en un llenguatge senzill i comprensible per a la persona interessada, de manera que li permeti fer-se una idea clara i precisa de l'abast del tractament de les dades i de les conseqüències que es deriven de facilitar-les.

No sempre cal facilitar el conjunt d'advertiments de l'article 5.1 de la LOPD. La mateixa norma ens indica que, quan el contingut de la informació es dedueixi clarament de la naturalesa de les dades que es demanen o de les circumstàncies en què es recullen, no cal facilitar la informació relativa a:

- el caràcter obligatori o facultatiu de la resposta a les preguntes.
- les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.
- la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.

El dret d'informació no regeix quan el fet d'informar-ne la persona interessada afecti la defensa nacional, la seguretat pública o la persecució d'infraccions penals.

Dades no recollides directament de la persona interessada

D'altra banda, encara que les dades no s'hagin recollit directament de la persona interessada, també cal facilitar el dret d'informació. En aquest cas, el responsable del fitxer ha d'informar de manera expressa, precisa i inequívoca a la persona interessada, en el termini de tres mesos des del moment en què s'han registrat les dades, de:

- el contingut del tractament
- la procedència de les dades

- l'existència d'un fitxer o un tractament de dades de caràcter personal, de la finalitat de la recollida de les dades i dels destinataris de la informació.
- la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.
- la identitat i l'adreça del responsable del tractament o, si s'escau, del seu representant.

Aquesta obligació no s'aplica quan:

- una llei ho prevegi expressament.
- el tractament tingui finalitats històriques, estadístiques o científiques.
- sigui impossible informar-ne la persona interessada o això exigeixi esforços desproporcionats, a criteri de l'Agència de Protecció de Dades, considerant el nombre de persones interessades, l'antiguitat de les dades o les mesures compensatòries aplicades.
- les dades provinguin de fonts accessibles al públic. No obstant això, en aquest supòsit caldrà informar en cada comunicació sobre l'origen de les dades, la identitat del responsable del tractament i els drets que pot exercir.

Acreditació del compliment del deure d'informació

L'article 18 del RLOPD estableix un conjunt d'obligacions respecte de la manera com s'ha d'acreditar que s'ha facilitat el dret d'informació:

- Cal complir el deure d'informació a través d'un mitjà que permeti acreditar-ne el compliment.
- Aquest mitja s'ha de conservar mentre persisteixi el tractament de les dades. El responsable del fitxer o tractament ha de conservar el suport en què consti el compliment del deure d'informar.

Per emmagatzemar els suports es poden utilitzar mitjans informàtics o telemàtics. En particular, s'indica que es pot escanejar la documentació en suport de paper, però cal que es garanteixi que en el procés d'automatització no s'ha produït cap alteració dels suports originals.

Consentiment de la persona afectada

Regla general: el tractament de dades personals exigeix el consentiment inequívoc de la persona interessada, llevat que una llei disposi una altra cosa.

Tot i l'establiment d'aquest principi a l'article 6.1 de la LOPD, en el segon apartat d'aquest mateix article s'estableixen un conjunt d'excepcions que, particularment, en el cas de les administracions públiques, comporta que la regla general es converteixi en l'excepció. Així, s'estableix que no cal el consentiment quan:

- Les dades de caràcter personal es recullin per a l'exercici de les funcions pròpies de les administracions públiques en l'àmbit de les seves competències.

- Les dades personals es refereixin a les parts d'un contracte o un precontracte d'una relació de negoci, laboral o administrativa i siguin necessàries per al seu manteniment o compliment.
- El tractament de les dades tingui com a finalitat protegir un interès vital de la persona interessada.
- Les dades figurin en fonts accessibles al públic i el seu tractament sigui necessari per a la satisfacció de l'interès legítim perseguit pel responsable del fitxer o pel del tercer a qui es comuniquin les dades.

No s'ha de confondre el dret d'informació amb el consentiment de la persona interessada. El dret d'informació, com hem vist, té poques excepcions i, en canvi, el principi del consentiment en té moltes.

D'altra banda, hem de tenir en compte que el consentiment obtingut per tractar les dades amb una finalitat determinada no comporta de manera directa el consentiment per a la seva cessió. Una cessió de dades és un nou tractament que requerirà l'obtenció d'un consentiment específic per dur-la a terme. Així, l'article 12.2 del RLOPD estableix que quan se sol·liciti el consentiment de la persona afectada per a la cessió de les seves dades, ha de ser informada de manera que conegui inequívocament la finalitat a què es destinaran les dades respecte de les quals se sol·licita el consentiment i el tipus d'activitat que porta a terme el cessionari.

En cas contrari, el consentiment és nul.

Finalment, cal recordar que correspon al responsable del tractament la prova de l'existència del consentiment de la persona afectada per qualsevol mitjà de prova admissible en dret.

Consentiment per al tractament de dades de menors

El RLOPD ha regulat, en l'article 13, quins són els requisits per procedir a la recollida i al tractament de dades de menors d'edat. Aquest article diferencia entre menors i majors de 14 anys.

Majors de 14 anys: se'ls pot demanar directament el seu consentiment, excepte en els casos en què la Llei exigeixi per a la seva prestació l'assistència dels titulars de la pàtria potestat o tutela.

Menors de 14 anys: per tractar les seves dades cal el consentiment dels pares o tutors. En aquest cas, es poden sol·licitar al menor les dades d'identitat i adreça del pare, mare o tutor amb l'única finalitat d'obtenir l'autorització per procedir al tractament de les dades del menor.

Límits en la recollida: No es poden demanar dades del menor que permetin obtenir informació sobre els altres membres de la família o sobre les característiques d'aquesta. No es poden demanar dades relatives, directa o indirectament, a l'activitat professional dels pares, informació econòmica, dades sociològiques o qualssevol altres.

La informació que es faciliti al menor en el procés d'obtenció del consentiment o en les clàusules informatives s'ha d'expressar en un llenguatge que els sigui fàcilment comprensible.

Consentiment i dades especialment protegides

Les dades especialment protegides o dades sensibles són les que revelen la ideologia, la religió, les creences, l'afiliació sindical i aquelles dades que es refereixen a l'origen racial, a la salut i a la vida sexual. Estan regulades a l'article 7 de la LOPD.

La LOPD, en aquest cas, estableix un tipus diferent de consentiment en funció de la naturalesa de les dades sensibles que es volen tractar. Així exigeix:

- Consentiment exprés i per escrit en el cas del tractament de les dades que revelen la ideologia, la religió, les creences, l'afiliació sindical. A més, en aquest cas, quan es recullen aquestes dades cal advertir a la persona interessada que no té l'obligació de facilitar-les.

No cal obtenir el consentiment per al tractament de les dades que revelin ideologia, religió, creences o afiliació sindical en els fitxers mantinguts pels partits polítics, els sindicats, les esglésies, les confessions o les comunitats religioses i associacions, les fundacions i altres entitats sense ànim de lucre, amb finalitat política, filosòfica, religiosa o sindical, quant a les dades relatives als seus associats o als seus membres, sens perjudici que la cessió d'aquestes dades requereix sempre el consentiment previ de la persona afectada.

- Consentiment exprés en el cas de les dades que es refereixen a l'origen racial, a la salut i a la vida sexual. Aquestes dades també es poden tractar quan una llei, per raons d'interès general, així ho estableixi.

En ambdós casos hem de fer notar que la LOPD no diu "dades de …", sinó dades que "revelin" o dades que es "refereixin", i això cal tenir-ho en compte en el moment de determinar si el tipus de dades que estem tractant són dades sensibles.

Queden prohibits els fitxers creats amb la finalitat exclusiva d'emmagatzemar dades de caràcter personal que revelin la ideologia, l'afiliació sindical, la religió, les creences, l'origen racial o ètnic o la vida sexual.

També es regulen dins l'article 7 de la LOPD les dades relatives a la comissió d'infraccions penals o administratives. En aquest cas, s'estableix que només poden ser incloses en els fitxers de les administracions públiques competents en els casos previstos en les normes que ho regulen.

Excepcions a l'obtenció del consentiment per al tractament de dades sensibles

L'apartat sisè de l'article 7 de la LOPD estableix un conjunt d'excepcions a la necessitat d'obtenir el consentiment en el tractament de les dades especialment protegides efectuat per un professional sanitari subjecte al secret professional o per una altra persona subjecta a una obligació equivalent de secret quan el tractament sigui necessari per a:

- la prevenció o per al diagnòstic mèdics,
- la prestació d'assistència sanitària o de tractaments mèdics,
- la gestió de serveis sanitaris.

També poden ser objecte de tractament les dades sensibles quan el tractament sigui necessari per salvaguardar l'interès vital de la persona afectada o d'una altra persona, en cas que la persona afectada estigui físicament o jurídicament incapacitada per donar-ne el consentiment.

Procediment per a l'obtenció del consentiment

L'article 14 RLOPD ha establert un procediment per a l'obtenció del consentiment de la persona interessada, tot i que en queden exceptuats aquells tractaments per als quals la legislació estableixi que cal obtenir el consentiment exprés per poder fer el tractament, com per exemple el cas de les dades especialment protegides regulades a l'article 7 de la LOPD.

Procediment:

- El responsable del fitxer s'ha de dirigir a la persona interessada i informar-la d'acord amb allò que estableix l'article 5 de la LOPD.
- Si també es vol obtenir el consentiment per portar a terme una cessió de dades, cal informar de manera inequívoca de la finalitat a la qual es destinaran les dades i del tipus d'activitat que realitza aquell a qui es cediran les dades.

Quan es tracti de responsables que prestin un servei a la persona afectada que generi informació periòdica o reiterada, o facturació periòdica, la comunicació es pot portar a terme de manera conjunta a aquesta informació o a la facturació del servei prestat, sempre que es faci de forma clarament visible.

- S'ha de donar a la persona interessada un termini de 30 dies per poder manifestar la seva negativa. Cal que se l'adverteixi que si no diu que no en aquest termini s'entén que està donant el seu consentiment al tractament i, si és el cas, a la cessió o les cessions de les quals s'informa.

S'ha de facilitar a la persona interessada un mitjà senzill i gratuït per manifestar la seva negativa al tractament de les dades. Per exemple, s'han de facilitar procediments en què la negativa es pugui efectuar mitjançant un enviament prefranquejat al responsable del tractament o mitjançant la trucada a un número telefònic gratuït o als serveis d'atenció al públic que el responsable hagi establert.

Per contra, no es considera un mitjà legítim per negar-se al tractament l'exigència d'enviar cartes certificades o similars, ni la utilització de serveis de telecomunicacions que impliquin una tarifació addicional a la persona afectada o qualsevol altre mitjà que impliqui un cost addicional a la persona interessada.

- El responsable del fitxer ha d'utilitzar un procediment que li permeti saber si la comunicació ha estat objecte de devolució. En aquest cas, no pot procedir al tractament.
- Si la persona interessada manifesta la seva negativa, el responsable del fitxer no pot tornar-li a demanar el consentiment respecte del mateix tractament i finalitats en el termini d'un any a comptar des de la data de l'anterior sol·licitud.

El RLOPD també ha regulat un supòsit especial que fins al moment havia generat nombrosos problemes: es regula com obtenir el consentiment de la persona interessada, en el marc d'una relació contractual, per a fins que no s'hi relacionin directament. En aquest cas, el responsable pot demanar el consentiment en el procés de formació del contracte per a finalitats que no tinguin una relació directa amb el manteniment, desenvolupament o control de la relació contractual, però ha de permetre a la persona afectada que manifesti expressament la seva negativa al tractament o comunicació de dades.

Per exemple, es pot obtenir el consentiment permetent a la persona interessada marcar una casella que ha d'estar clarament visible i que no pot venir marcada en el document que se li lliuri per a la subscripció del contracte.

Aquesta previsió seria aplicable al supòsit regulat a l'article 14 del RLOPD quan la sol·licitud de consentiment es refereix a diferents finalitats, tractaments o cessions, en què s'hauria de permetre negar-se de manera individualitzada a cada tractament.

Revocació del consentiment

El consentiment es pot revocar sempre que hi hagi una causa justificada. La revocació no té efectes retroactius.

El responsable del fitxer ha d'establir un mitjà senzill per tal que la persona interessada pugui revocar el consentiment, com per exemple, mitjançant un enviament prefranquejat al responsable del tractament o la trucada a un número telefònic gratuït o als serveis d'atenció al públic que aquest responsable ha establert.

D'altra banda, en aquells supòsits en què per portar a terme un determinat tractament no sigui necessari el consentiment, la persona afectada s'hi pot oposar, tal com es veurà en el mòdul 4, en què es tractarà la regulació dels drets d'accés, rectificació, cancel·lació i oposició.

Des de la recepció de la revocació del consentiment o de l'exercici de l'oposició, el responsable del tractament té 10 dies per fer cessar el tractament. A més, si la persona interessada ha demanat que se li confirmi que ja no es porta a terme aquest tractament, el responsable li ha de respondre expressament.

Si les dades respecte de les quals s'ha revocat el consentiment havien estat cedides a tercers, el responsable del tractament ha de comunicar la revocació als cessionaris, en el termini de 10 dies, perquè posin fi al tractament de les dades.

Comunicació de dades personals

La cessió de les dades personals

La cessió o comunicació de dades personals està definida a l'article 3.i) de la LOPD com qualsevol revelació de dades efectuada a una persona diferent de la persona interessada, és a dir, a una persona diferent de la persona física titular de les dades.

Hem de tenir en compte que la cessió de dades comporta, per a la persona interessada, una important pèrdua de control sobre les seves dades personals, atès que la informació passa a entitats o persones diferents d'aquelles a qui, en principi, ella ha facilitat les dades. És per això que pren especial importància respecte d'aquest fet la informació i la transparència quant als destinataris de la informació.

El **règim general de la cessió** de dades s'estableix a l'article 11 de la LOPD. Així, per tal de portar a terme una comunicació de dades, cal:

- Que la cessió de dades tingui per objecte el compliment de finalitats directament relacionades amb les funcions legítimes de l'entitat que cedeix les dades (cedent) i de qui les rep (cessionari).
- Obtenir prèviament el consentiment de la persona titular de les dades.

Aquest mateix article estableix, en el punt 2, una sèrie d'**excepcions** a la necessitat d'obtenir el **consentiment previ** de la persona titular de les dades. Aquestes excepcions són les següents:

1. Quan la cessió està autoritzada en una llei.
2. Quan es tracti de dades recollides de fonts accessibles al públic.
3. Quan el tractament respongui a la lliure i legítima acceptació d'una relació jurídica el desenvolupament, el compliment i el control de la qual impliqui necessàriament la connexió del tractament esmentat amb fitxers de tercers. En aquest cas, la comunicació només és legítima quan es limiti a la finalitat que la justifiqui.

4. Quan la comunicació que s'hagi d'efectuar tingui com a 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.
5. Quan la comunicació tingui com a destinatari institucions autonòmiques amb funcions anàlogues al defensor del Poble o al Tribunal de Comptes.
6. Quan la cessió es produeixi entre administracions públiques i tingui com a objecte el tractament posterior de les dades amb finalitats històriques, estadístiques o científiques.
7. Quan la cessió de dades de caràcter personal relatives a la salut sigui necessària per solucionar una urgència que requereixi accedir a un fitxer o per fer els estudis epidemiològics en els termes que estableix la legislació sobre sanitat estatal o autonòmica.

L'aplicació de qualsevol d'aquestes excepcions ha de fer-se sempre utilitzant un **criteri restrictiu** i aplicant els **principis de qualitat** establerts a l'article 4 de la LOPD.

En aquells supòsits en què sigui necessària l'obtenció del consentiment (per tant, informat) o, si no és el cas, quan es faciliti el dret d'informació, hem de tenir present que cal que la persona interessada pugui conèixer la **finalitat** a què es destinaran les dades cedides o el **tipus d'activitat** del receptor de la comunicació. En cas contrari, el consentiment serà nul.

D'altra banda, el consentiment pot ser revocat en qualsevol moment, tot i que aquesta **revocació** no té efectes retroactius.

Quant a les **obligacions del cessionari**, és important recordar l'article 11.5 de la LOPD, en què s'estableix que el cessionari queda subjecte al compliment del conjunt d'obligacions establertes a la normativa de protecció de dades pel sol fet de la comunicació. Tot i que aquesta afirmació pugui semblar evident quant als tractaments posteriors que es realitzin amb les dades, també es refereix a la legitimitat de la recollida, és a dir: el cessionari té l'obligació de comprovar que el cedent està legitimat per realitzar la cessió de les dades, com per exemple -si és el cas-, que ha obtingut el pertinent consentiment previ.

Finalment, cal indicar que en el cas de cessió **de dades de fitxers de titularitat privada**, el responsable del fitxer, en el moment en què s'efectuï la primera cessió de dades, ha d'informar-ne les persones afectades i els ha de comunicar la finalitat del fitxer, la naturalesa de les dades que han estat cedides i el nom i l'adreça del cessionari.

En cas que la cessió vingui imposada per llei, aquesta obligació no existeix en els supòsits següents:

- Quan el tractament respongui a la lliure i legítima acceptació d'una relació jurídica el desenvolupament, el compliment i el control de la qual impliqui necessàriament la connexió del tractament esmentat amb fitxers de tercers. En aquest cas, la comunicació només és legítima quan es limiti a la finalitat que la justifiqui.
- Quan la comunicació que s'hagi d'efectuar tingui com a 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 cal el consentiment quan la comunicació tingui com a destinatari institucions autonòmiques amb funcions anàlogues al defensor del Poble o al Tribunal de Comptes.
- Quan la cessió es produeixi entre administracions públiques i tingui com a objecte el tractament posterior de les dades amb finalitats històriques, estadístiques o científiques.
- Si la comunicació s'efectua amb el procediment previ de dissociació.

Comunicacions de dades entre administracions públiques

A banda del que regula l'article 11.2 d) de la LOPD, respecte a la possibilitat que tenen les administracions públiques de comunicar-se dades sense el consentiment de la persona

interessada quan això tingui com a objecte el tractament posterior de les dades amb finalitats històriques, estadístiques o científiques, la LOPD estableix una regulació especial a l'article 21, segons el qual les administracions públiques es poden comunicar dades sense el consentiment de la persona interessada sempre que sigui per a:

- l'exercici de les mateixes competències.
- l'exercici de competències que es refereixin a les mateixes matèries.
- el tractament posterior de les dades amb finalitats històriques, estadístiques o científiques.

D'altra banda, també es poden comunicar les dades personals que una administració pública obtingui o elabori amb destinació a una altra.

Així mateix, s'estableix la prohibició de cedir a fitxers de titularitat privada, sense el consentiment de la persona interessada, les dades recollides de fonts accessibles al públic.

Comunicació de dades especialment protegides

Les dades especialment protegides o dades sensibles estan regulades a l'article 7 de la LOPD i són les dades relatives a:

1. la ideologia, l'afiliació sindical, la religió i les creences.
2. l'origen racial, la salut i la vida sexual.

En el primer cas, només es poden cedir les dades amb el consentiment exprés i per escrit de les persones interessades.

En el segon cas, es poden cedir les dades quan:

- una llei ho estableixi, per raons d'interès general, o
- la persona afectada hi consenti expressament.

En tot cas, es poden cedir aquests tipus de dades quan el tractament sigui necessari per a:

- la prevenció o per al diagnòstic mèdics
- la prestació d'assistència sanitària o de tractaments mèdics
- la gestió de serveis sanitaris.

En aquests casos, però, el tractament l'ha d'efectuar un professional sanitari subjecte al secret professional o una altra persona subjecta a una obligació equivalent de secret.

D'altra banda, també poden ser objecte de tractament aquestes dades quan això sigui necessari per salvaguardar l'interès vital de la persona afectada o d'una altra persona, en cas que l'afectada estigui físicament o jurídicament incapacitada per donar-ne el consentiment.

Transferències internacionals

El RLOPD ha definit les transferències internacionals a l'article 5.s) com:

Tot tractament de dades que suposa una transmissió d'aquestes dades fora del territori de l'Espai Econòmic Europeu, tant si constitueix una cessió o comunicació de dades, com si té per objecte la realització d'un tractament de dades per compte del responsable del fitxer establert en el territori espanyol.

Per tal d'analitzar les transferències internacionals hem de diferenciar tres **tipus de països**:

- Països que són dins l'Espai Econòmic Europeu. En aquest cas el RLOPD considera que no existeix una transferència internacional. Cal, en tot cas, aplicar el règim de protecció de dades establert a la LOPD i la normativa que la desenvolupa.
- Països que garanteixen un nivell de protecció equiparable al de la LOPD. En aquest cas es podrà portar a terme la transferència internacional si es compleixen els requisits generals establerts a la LOPD. En són exemple els països respecte del quals la Comissió Europea ha declarat que tenen un nivell de protecció adequat.
- Països que no garanteixen un nivell de protecció equiparable al de la LOPD. En aquest cas caldrà:
  1. Sol·licitar l'autorització prèvia de l'Agència de Protecció de Dades.
  2. Complir amb el requisits establerts a la LOPD.

Per tal de determinar l'adequació del **nivell de protecció** del país de destinació és tindrà en compte:

- la naturalesa de les dades
- la finalitat del tractament
- la durada del tractament
- el país d'origen i el país de destinació final
- les normes de dret, generals o sectorials, vigents en el país de destinació
- el contingut dels informes de la Comissió de la Unió Europea
- les normes professionals i les mesures de seguretat en vigor al país de destinació.

L'**autorització** es pot atorgar si:

- El responsable del fitxer aporta un contracte subscrit entre aquell que realitza la transferència i aquell que en rep les dades que inclogui les garanties necessàries per protegir la vida privada de les persones i el conjunt de drets i llibertats fonamentals. Les decisions de la Comissió Europea 2001/497/CE, de 15 de juny de 2001, 2002/16/CE, de 27 de desembre de 2001, i 2004/915/CE, de 27 de desembre de 2004, estableixen les garanties que es consideren adequades a aquests efectes.
- La transferència es produeix al si de grups multinacionals d'empreses que hagin adoptat normes o regles internes en què constin les garanties necessàries de respecte per al dret a la protecció de dades personals i es garanteix el compliment dels principis i l'exercici dels drets de la LOPD. En aquest cas, és necessari que les normes o regles siguin vinculants per a les empreses del grup i exigibles conforme a l'ordenament jurídic espanyol.

En tot cas, l'Agència pot **suspendre** la transferència internacional en els suposits establerts a l'article 70.3 del RLOPD.

Tot i aquest règim general, la LOPD estableix una sèrie d'**excepcions** que permeten la transferència internacional tot i que no es garanteixi un nivell de protecció equiparable:

- Quan la persona afectada hagi donat el seu consentiment inequívoc a la transferència prevista.
- Quan la transferència internacional de dades de caràcter personal resulti de l'aplicació de tractats o convenis en què Espanya sigui part.
- Quan la transferència es faci a efectes de prestar o sol·licitar auxili judicial internacional.
- Quan la transferència sigui necessària per a la prevenció o per al diagnòstic mèdics, la prestació d'assistència sanitària o tractament mèdics o la gestió de serveis sanitaris.
- Quan es refereixi a transferències dineràries, d'acord amb la legislació específica.

- Quan la transferència sigui necessària per a l'execució d'un contracte entre la persona afectada i el responsable del fitxer o per a l'adopció de mesures precontractuals adoptades a petició de la persona afectada.
- Quan la transferència sigui necessària per a la subscripció o l'execució d'un contracte subscrit o per subscriure pel responsable del fitxer i un tercer, en interès de l'afectat.
- Quan la transferència sigui necessària o legalment exigida per salvaguardar un interès públic. Té aquesta consideració la transferència sol·licitada per una administració fiscal o duanera per al compliment de les seves competències.
- Quan la transferència sigui necessària per al reconeixement, l'exercici o la defensa d'un dret en un procés judicial.
- Quan la transferència s'efectuï, a petició d'una persona amb interès legítim, des d'un registre públic i aquella estigui d'acord amb la finalitat del registre.
- Quan la transferència tingui com a destinació 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.

Creació de fitxers

Fitxers de titularitat pública

Són fitxers de titularitat pública els fitxers els responsables dels quals siguin els òrgans constitucionals o amb rellevància constitucional de l'Estat o les institucions autonòmiques amb funcions anàlogues a aquests òrgans, les administracions públiques territorials, així com les entitats o organismes que hi estan vinculats o en depenen i les corporacions de dret públic, sempre que la seva finalitat sigui l'exercici de potestats de dret públic (article 5.m) del RLOPD).

El Capítol I del Títol IV de la LOPD estableix una sèrie de disposicions sectorials relatives als fitxers de titularitat pública respecte de:

- La creació, modificació i supressió de fitxers, que en el cas dels fitxers de titularitat pública s'ha de fer mitjançant una disposició de caràcter general o acord. Les disposicions de creació o de modificació han d'indicar:
  - La finalitat del fitxer i els usos previstos.
  - Les persones o els col·lectius sobre els quals es pretén obtenir dades de caràcter personal o que estiguin obligats a subministrar-les.
  - El procediment de recollida de les dades de caràcter personal.
  - L'estructura bàsica del fitxer i la descripció dels tipus de dades de caràcter personal incloses en aquest fitxer.
  - Les cessions de dades de caràcter personal i, si s'escau, les transferències de dades que es prevegin a països tercers.
  - Els òrgans de les administracions responsables del fitxer.
  - Els serveis o les unitats davant els quals es puguin exercir els drets d'accés, rectificació, cancel·lació i oposició.
  - Les mesures de seguretat amb indicació del nivell bàsic, mitjà o alt exigible.
  - La procedència de les dades.
  - El sistema de tractament utilitzat en l'organització.

(Els dos últims punts han estat afegits pel RLOPD.)

En les disposicions que es dictin per a la supressió dels fitxers, se n'ha d'establir el destí o, si s'escau, les previsions que s'adoptin per destruir-los.

- Les comunicacions de dades entre administracions públiques. Aquest aspecte ha estat desenvolupat al punt 5 d'aquesta unitat.
- Els fitxers de les Forces i Cossos de Seguretat.
- Les excepcions al dret d'informació i als drets d'accés, rectificació i cancel·lació. Aquestes qüestions es desenvolupen a la unitat 4.

Tots aquests punts són tractats amb detall al llarg del curs, excepte el que fa referència als fitxers de les Forces i Cossos de Seguretat, respecte del qual introduirem unes notes breus.

Fitxers de les Forces i Cossos de Seguretat

En aquest àmbit podem diferenciar dos tipus de fitxers:

1. Els fitxers amb finalitats administratives, als quals s'aplica el règim general de la LOPD.
2. Els fitxers amb finalitats policials. En aquest cas, s'estableixen una sèrie d'excepcions al consentiment de la persona interessada.

Amb caràcter general, la recollida i el tractament de dades personals amb finalitats policials es pot portar a terme sense el consentiment de la persona titular de les dades quan es donin les circumstàncies següents:

- Supòsits i categories de dades que siguin necessaris per a la prevenció d'un perill real per a la seguretat pública o per a la repressió d'infraccions penals.
- Les dades estan emmagatzemades en fitxers específics establerts a aquest efecte.
- Les dades estan classificades per categories d'acord amb el grau de fiabilitat.

Quant a la recollida i el tractament de dades especialment protegides, només es pot realitzar quan sigui absolutament necessari per a les finalitats d'una investigació concreta.

La LOPD també ha pres en consideració les particularitats d'aquest tipus de tractaments en relació amb el temps de conservació de les dades i recorda el principi establert a l'article 4 de la mateixa Llei, segons el qual les dades personals s'han de cancel·lar quan no siguin necessàries per a les investigacions que n'hagin motivat l'emmagatzematge. La mateixa Llei enumera allò que s'ha de tenir en compte als efectes de determinar les dades que s'han cancel·lar:

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

Fitxers de titularitat privada

Són fitxers de titularitat privada els fitxers els responsables dels quals siguin les persones, empreses o entitats de dret privat, amb independència de qui tingui la titularitat del seu capital o de la procedència dels seus recursos econòmics, així com els fitxers els responsables dels quals siguin les corporacions de dret públic, si és que aquests fitxers no estan estrictament vinculats a

l'exercici de potestats de dret públic que els atribueix la seva normativa específica (article 5 l) RLOPD).

La LOPD estableix, a l'article 25, la legitimitat per crear fitxers de titularitat privada i indica que es poden crear quan sigui necessari per aconseguir l'activitat o l'objecte legítims de la persona, l'empresa o l'entitat titular i es respectin les garanties que estableix la mateixa LOPD.

Un cop creat el fitxer, cal notificar-lo al registre de protecció de dades de l'agència de protecció de dades competent conforme al bloc de constitucionalitat.

En el cas de Catalunya, per determinar quins són els fitxers de titularitat privada que queden subjectes al control de l'Agència Catalana de Protecció de Dades, caldrà atenir-se al que estableix l'article 156 de l'Estatut d'Autonomia de Catalunya.

La LOPD i el RLOPD regulen de manera específica determinats tipus de fitxers de titularitat privada que comporten un risc especial per al dret a la protecció de dades personals i que han generat nombroses consultes i denúncies. Ens referim als fitxers per a la prestació de serveis d'informació sobre solvència patrimonial i crèdit i als tractaments amb finalitats de publicitat i de prospecció comercial.

Inscripció de fitxers

Directiva 95/46/CE del Parlament Europeu i del Consell

L'obligació de la notificació dels fitxers es recull a la **Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades**. Els Estats membres han d'establir que el responsable del tractament efectuï una notificació a l'autoritat de control. Aquest mateix precepte recull els supòsits de simplificació, omissió i exempció de la notificació.

D'altra banda, la directiva atribueix igualment als Estats membres:

- l'establiment de controls previs de l'existència de riscos per als drets i les llibertats de les persones interessades, per tal que puguin ser examinats abans de l'inici del tractament, i
- l'adopció de les mesures necessàries per garantir la publicitat dels tractaments i establir que l'autoritat de control gestioni un registre dels tractaments notificats.

Regulació a la Llei orgànica de protecció de dades de caràcter personal i al Reglament que la desplega

Les previsions de la directiva es van incorporar a la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, la qual determina, en relació amb els *fitxers de titularitat pública*, que la creació, la modificació o la supressió dels fitxers de les administracions públiques només es poden fer per mitjà d'una disposició de caràcter general publicada en el Butlletí Oficial de l'Estat o en el diari oficial corresponent. *Els fitxers de titularitat privada* s'han de notificar amb caràcter previ a la seva creació. La notificació ha de contenir els mateixos elements que la disposició de creació dels fitxers de titularitat pública i la informació s'ha de mantenir actualitzada.

Pel que fa al registre, la Llei orgànica de protecció de dades de caràcter personal, d'una banda, regula el *Registre General de Protecció de Dades* i, de l'altra, atribueix a les comunitats autònomes la possibilitat de crear i mantenir els seus propis registres de fitxers per a l'exercici de les competències que se'ls reconeix sobre aquests.

Regulació a la Llei de l'Agència Catalana de Protecció de Dades

Mitjançant la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades, es va crear el *Registre de Protecció de Dades de Catalunya*, com a òrgan integrat a l'Agència. Segons aquesta Llei, al Registre de Protecció de Dades de Catalunya s'hi han d'inscriure:

a) Els fitxers de dades personals inclosos en l'àmbit d'aplicació de la Llei orgànica de protecció de dades de caràcter personal, que siguin de titularitat de la Generalitat de Catalunya, dels ens que integren l'Administració local en l'àmbit territorial de Catalunya i de la resta d'organismes i entitats sobre els quals l'Agència exerceix la seva activitat de control (universitats de l'àmbit territorial de Catalunya; organismes i entitats autònomes que depenen de l'Administració de la Generalitat o dels ens locals, i consorcis dels quals formen part; entitats prestadores de serveis públics, associacions, fundacions, societats civils i societats mercantils en les quals la Generalitat o els ens locals tinguin la participació majoritària del capital, quan porten a terme activitats per compte d'una administració pública), i també les dades relatives a aquests fitxers que siguin necessàries per a l'exercici dels drets d'informació, d'accés, de rectificació, de cancel·lació i d'oposició.

b) Els codis tipus definits per la Llei orgànica de protecció de dades de caràcter personal formulats per la Generalitat de Catalunya o pels ens que integren l'Administració local en l'àmbit territorial de Catalunya.

L'Estatut d'autonomia de Catalunya

Article 156. Protecció de dades de caràcter personal

Correspon a la Generalitat la competència executiva en matèria de protecció de dades de caràcter personal que, respectant les garanties dels drets fonamentals en aquesta matèria, inclou en tot cas:

***a)** La inscripció i el control dels fitxers o els tractaments de dades de caràcter personal creats o gestionats per les institucions públiques de Catalunya, l'Administració de la Generalitat, les administracions locals de Catalunya, les entitats autònomes i les altres entitats de dret públic o privat que depenen de les administracions autonòmica o locals o que presten serveis o acompleixen activitats per compte propi per mitjà de qualsevol forma de gestió directa o indirecta, i les universitats que integren el sistema universitari català.*

***b)** La inscripció i el control dels fitxers o els tractaments de dades de caràcter personal privats creats o gestionats per persones físiques o jurídiques per a l'exercici de les funcions públiques amb relació a matèries que són competència de la Generalitat o dels ens locals de Catalunya, si el tractament s'efectua a Catalunya.*

***c)** La inscripció i el control dels fitxers i els tractaments de dades que creïn o gestionin les corporacions de dret públic que exerceixin llurs funcions exclusivament en l'àmbit territorial de Catalunya.*

***d)** La constitució d'una autoritat independent, designada pel Parlament, que vetlli per garantir el dret a la protecció de les dades personals en l'àmbit de les competències de la Generalitat.*

Així, doncs, correspon a la Generalitat la inscripció dels fitxers creats o gestionats per:

- Les institucions públiques de Catalunya (el Parlament, el president o presidenta de la Generalitat, el Govern i l'Administració de la Generalitat, el Consell de Garanties Estatutàries, el síndic o síndica de greuges, la Sindicatura de Comptes, el Consell de l'Audiovisual de Catalunya…).
- L'Administració de la Generalitat i les entitats autònomes i entitats de dret públic o privat que en depenen.
- Les administracions locals i les entitats autònomes i entitats de dret públic o privat que en depenen.
- Les entitats que presten serveis o acompleixen activitats per compte propi per mitjà de qualsevol forma de gestió directa o indirecta (concessionàries).
- Les universitats que integren el sistema universitari català.

•Les persones físiques o jurídiques per a l'exercici de funcions públiques amb relació a matèries que són competència de l'Administració de la Generalitat, si el tractament s'efectua a Catalunya.

•Les persones físiques o jurídiques per a l'exercici de funcions públiques amb relació a matèries que són competència de les administracions locals, si el tractament s'efectua a Catalunya.

•Les corporacions de dret públic que exerceixin llurs funcions exclusivament en l'àmbit territorial de Catalunya (col·legis professionals; consells de col·legis professionals; cambres de comerç, indústria i navegació; comunitats d'usuaris de la llei d'aigües; consells reguladors de les denominacions d'origen).

Procediment d'inscripció

Fitxers que s'han de notificar: qualsevol fitxer (*conjunt organitzat de dades, sigui quina sigui la forma o la modalitat de creació, emmagatzematge, organització i accés*) amb dades personals, automatitzat, no automatitzat o parcialment automatitzat, que formi part de l'àmbit d'aplicació de l'Agència Catalana de Protecció de Dades.

Pel que fa als *tipus d'inscripcions*, aquestes poden ser de creació, de modificació o de supressió.

L'obligació de notificar recau en el responsable del fitxer, que és la persona física o jurídica, de naturalesa pública o privada, o l'òrgan administratiu, que decideixi sobre la finalitat, el contingut i l'ús del tractament.

Inici: amb la notificació de la creació, modificació o supressió del fitxer per part de l'interessat, mitjançant els models de sol·licitd i de formularis aprovats per l'Agència Catalana de Protecció de Dades (Resolució de 15 de desembre de 2003, modificada per la Resolució de 23 de juny de 2004, i Resolució de 16 de desembre de 2008).

Termini per resoldre: el termini màxim per dictar i notificar la resolució sobre la inscripció, modificació o cancel·lació és d'un mes, de manera que si en aquest termini no s'ha dictat resolució expressa, el fitxer s'entén inscrit, modificat o cancel·lat a tots els efectes.

Infraccions

La Llei orgànica de protecció de dades de caràcter personal tipifica:

•Com a infracció lleu: no sol·licitar la inscripció del fitxer de dades de caràcter personal al registre, quan no sigui constitutitva d'infracció greu.

•Com a infracció greu: no inscriure el fitxer de dades de caràcter personal al registre, quan hi hagi hagut un requeriment per fer-ho.

Unitat 4: Potestats d'exercici del dret a la protecció de dades

Drets ARCO (Accés, Rectificació, Cancel·lació, Oposició)

Disposicions comunes

Quan parlem dels drets ARCO ens referim als drets d'accés, rectificació, cancel·lació i oposició. Aquests drets estan regulats als articles que van del 15 al 18 de la LOPD i, de manera més detallada, als articles que van del 23 al 36 del RLOPD. A aquests articles s'hi poden afegir d'altres del RLOPD dedicats a alguns supòsits específics, com ara els articles 37.2 i 44, sobre els fitxers d'informació sobre solvència patrimonial i crèdit, o l'article 50, per a les activitats de publicitat i prospecció comercial.

Els drets esmentats els trobem al nucli del dret fonamental a la protecció de dades de caràcter personal, que "persegueix garantir a la persona un poder de control sobre les seves dades personals, sobre el seu ús i la seva destinació, amb el propòsit d'impedir el seu tràfic il•lícit i lesiu per a la dignitat i el dret de l'afectat" (STC 292/2000). A més, en aquesta mateixa STC 292/2000 es reprodueix novament allò que ja s'havia declarat en l'STC 254/1993: "el dret a la protecció de dades atribueix a la persona que n'és titular un conjunt de facultats consistents en diversos poders jurídics, l'exercici dels quals imposa a tercers deures jurídics (…)". I entre aquestes facultats, el TC destaca el dret a accedir, rectificar i cancel·lar les dades personals, en definitiva: el poder de disposició sobre les dades personals, o el que s'anomena l'autodeterminació informativa.

Els **Drets ARCO** són els drets d'accés, rectificació, cancel•lació i oposició, drets també denominats com d'*habeas data.*

Condicions generals per a l'exercici dels drets ARCO

El RLOPD precisa que l'exercici dels drets ARCO és independent, de manera que no cal exercir cap dret com a requisit previ d'un altre. És a dir, per exercir el dret de rectificació o cancel•lació no cal exercir prèviament el dret d'accés. Això no vol dir que en ocasions no sigui necessari exercir primer el dret d'accés i, un cop vist el contingut del document o suport que conté la dada personal, demanar la cancel•lació, rectificació o oposició.

L'article 24.2 del RLOPD disposa que per a l'exercici dels drets ARCO s'ha de concedir a la persona interessada un mitjà senzill i gratuït. L'article 24.3, també del RLOPD, insisteix a dir que l'exercici dels drets ARCO ha de ser gratuït i en cap cas pot implicar un ingrés addicional. Ara bé, per molt que es repeteixi aquest caràcter de gratuïtat, el significat no és el de garantir un cost zero, sinó que el responsable del fitxer no pot exigir una contraprestació econòmica per tal de facilitar l'exercici del dret, tal com advertia ja la mateixa LOPD a l'article 17.2. Per tant, l'eventual cost ha de ser reduït. Es tracta del mateix cas que es produeix amb els procediments administratius, en els quals regeix la regla de la gratuïtat, però això no impedeix que s'hagin de suportar algunes despeses, com ara enviar escrits per correu certificat o fer desplaçaments a un registre. En aquesta línia, el RLOPD disposa que seria contrari a la LOPD implantar un sistema via telèfon amb tarificació addicional o a través de cartes certificades. Sobre les cartes certificades, potser no és conforme a la LOPD exigir que la persona afectada utilitzi aquest mitjà, però la realitat és que, si la persona no té al seu abast l'opció telemàtica amb signatura electrònica, potser el correu certificat és la via més adequada si el que vol és tenir constància del dret exercit, perquè si utilitza un sobre prefranquejat o el correu ordinari i el responsable del fitxer nega haver rebut res, la persona afectada tindrà un problema de prova.

En cas que el responsable del fitxer tingui serveis d'atenció al públic (per exemple, el cas d'operadors de telecomunicacions), l'article 24.4 del RLOPD permet articular els drets ARCO a través d'aquests mitjans, i afegeix que es pot entendre acreditada la identitat de la persona afectada pels mateixos sistemes que s'admeten per a la contractació. És a dir, si per contractar el servei (per exemple, la línia telefònica) s'admet la identificació mitjançant el reconeixement de veu, també serà vàlid aquest sistema per exercir els drets ARCO. Aquesta equiparació és d'una lògica indiscutible i semblaria innecessària fer aquesta precisió, però convé fer-la, sobretot després d'haver pogut constatar les diferents maneres d'actuar si la gestió que es fa és, per exemple, una alta o bé si es tracta d'altres gestions que ja no agraden tant a l'empresa. En aquest punt, s'ha de tenir en compte també l'article 2 de la Llei 56/2007, de mesures d'impuls de la societat de la informació, aprovada el mateix dia que el RLOPD, el qual disposa que las empreses que presten serveis al públic en general de transcendència econòmica especial estan obligades a facilitar als usuaris un mitjà d'interlocució telemàtic amb certificats reconeguts que permeti fer, entre altres tràmits, els d'exercici dels drets ARCO. També la Llei 34/2002, de serveis de la societat de la informació i comerç electrònic, disposa a l'article 21, en regular les comunicacions comercials electròniques, que s'ha d'oferir al destinatari la possibilitat d'oposar-se al tractament de les seves dades amb finalitats promocionals, mitjançant un procediment senzill i gratuït.

Aquest article conclou amb l'advertència que s'ha d'admetre la sol•licitud dels drets ARCO quan la persona afectada no utilitza el procediment establert a aquest efecte, sempre que el mitjà utilitzat permeti acreditar l'enviament i la recepció de la sol•licitud.

Procediment d'exercici dels drets ARCO

L'article 17 de la LOPD es refereix al procediment d'exercici dels drets ARCO, però al marge d'advertir que en cap cas no es pot exigir una contraprestació econòmica, no en regula el procediment, sinó que el difereix al seu desenvolupament reglamentari. La regulació del procediment la tenim a l'article 25 del RLOPD, precepte que configura el mitjà escrit com a habitual per exercir els drets ARCO, tret del cas que hem vist d'empreses que disposen de serveis d'atenció al públic o de les que presten serveis al públic de transcendència econòmica especial, les quals han de permetre fer-ho per via telemàtica conforme a la Llei 56/2007, tot i que l'opció de la signatura electrònica encara queda una mica lluny per a molts ciutadans o, si més no, hi quedava en el moment d'entrada en vigor del RLOPD.

El mateix article 25 del RLOPD relaciona els requisits que ha de tenir la sol•licitud d'exercici dels drets ARCO i, en cas que no els reuneixi, obliga a donar la possibilitat d'esmena. El RLOPD no ho diu expressament, però per a les sol·licituds formulades davant les administracions públiques aquesta petició d'esmena hauria de tenir la forma de requeriment que disposa l'article 71 de la LRJPA i concedir un termini de 10 dies, amb l'advertiment que si no s'esmena la sol•licitud d'exercici de drets ARCO, es tindrà per desistida .

Pel que fa a l'exercici d'aquests drets respecte a dades personals consistents en imatges captades per càmeres de vídeo o altres d'equivalents, el RLOPD no conté cap previsió específica, però per tal de facilitar la identificació de la persona que exerceix el dret caldria aportar una imatge actualitzada, tal com disposa la Instrucció 1/2009 de l'APDCAT i també la Instrucció 1/2006 de l'AEPD.

Les sol•licituds ARCO s'han de contestar sempre de forma expressa, encara que només sigui per dir que no es pot fer efectiu el dret perquè no existeix en el fitxer cap dada personal de la persona sol•licitant (article 25.2 del RLOPD), i en tot cas la resposta s'ha d'efectuar per un mitjà que permeti tenir-ne constància i ha de conservar-se l'acreditació (article 25.5 de la RLOPD).

Així doncs, l'article 25.5 del RLOPD imposa la càrrega de la prova al responsable del fitxer, el qual haurà de poder acreditar que ha donat resposta, però el problema és que abans recau sobre la persona afectada la prova d'acreditar que ha exercit el dret.

L'article 25.6 RLOPD imposa al responsable una obligació més, que és la de garantir que els empleats que tenen accés a dades personals estiguin suficientment formats com per poder informar les persones interessades sobre el procediment per exercir els drets ARCO. No sembla que s'hagi d'interpretar el precepte de manera literal, cosa que obligaria que tots els empleats que tracten dades estiguessin en condicions d'oferir aquesta informació, sinó que sembla més lògic entendre que l'obligació recau sobre aquells empleats que poden tenir contacte amb les persones afectades, com seria el cas, per exemple, dels serveis d'atenció al públic.

L'article 25.7 del RLPD permet modular els drets ARCO, per raons de seguretat pública, en els casos i amb l'abast previstos a les lleis. La mateixa LOPD preveu a l'article 23, per a determinats fitxers públics, excepcions a l'exercici dels drets en casos de perill per a la defensa de l'estat o seguretat pública, protecció de tercers o necessitats de les investigacions que s'estiguin duen a terme. També és procedent aquesta modulació en l'àmbit de la hisenda pública, en els casos en què l'exercici del dret pugui obstaculitzar les actuacions administratives tendents a assegurar el compliment de les obligacions tributàries i, en tot cas, quan la persona afectada és objecte d'actuacions inspectores. És oportú recordar, en aquest punt, que l'article 24.2 de la LOPD havia previst, també en relació amb els fitxers públics, unes restriccions a l'exercici dels drets ARCO que es van declarar inconstitucionals per l'STC 292/2000, perquè no era la pròpia llei la que fixava el límit al dret, sinó que remetia aquesta facultat a les administracions públiques a través de la disposició general de creació del fitxer.

L'article 25.8 del RLOPD fa referència als drets de cancel•lació i rectificació en casos especials, en què se segueix el procediment de la norma sectorial. És una remissió a la normativa sectorial molt oberta, però només per als drets de rectificació o cancel•lació. Es refereix a casos de registres específics com poden ser el registre civil, el de la propietat o també registres d'infraccions administratives o d'antecedents penals.

El caràcter personalíssim dels drets ARCO

Tots els drets ARCO tenen caràcter personalíssim (article 23 del RLOPD), la qual cosa significa que només els pot exercir la persona afectada. Aquesta exigència és lògica, ja que si parlem del dret a l'autodeterminació informativa, és a dir al fet que cada persona tingui un poder de disposició sobre les seves dades personals, és obvi que només ella mateixa sigui qui ha d'administrar aquest poder.

Això no vol dir que els drets ARCO no es puguin exercir a través de representant, ja que el mateix RLOPD preveu aquesta possibilitat a l'article 23.2. Ara bé, caldrà que aquesta representació s'acrediti documentalment.

En primer lloc, quan la persona afectada estigui en situació d'incapacitat o minoria d'edat que la impossibiliti per a l'exercici personal d'aquests drets, d'acord amb l'article 23.2.b) del RLOPD, el seu representant legal pot exercir-los havent acreditat prèviament aquesta representació, la qual podem qualificar de forçosa.

D'altra banda, l'article 23.2.c) del RLOPD fa referència a la representació voluntària, supòsit en el qual la persona afectada no està incapacitada, però actua mitjançant una persona que la representa. Referent a això, el RLOPD regula per separat l'acreditació d'aquesta representació voluntària segons si s'exerceix davant d'entitats públiques o de privades.

Davant d'entitats privades, el RLOPD preveu a l'article 23.2.c) una sola forma d'acreditar la representació, que consisteix a aportar una còpia del DNI i la representació conferida per la persona afectada, cosa que permet entendre que es pot fer amb una simple declaració amb la signatura de la persona afectada, de forma semblant a com autoritzem la representació per recollir un certificat a correus.

En canvi, per al cas d'administracions públiques, els segon paràgraf de l'article 23.2.c) del RLOPD transcriu pràcticament l'article 32 de la LRJPA i exigeix l'acreditació de la representació per qualsevol mitjà vàlid en dret que en deixi constància fidedigna, o mitjançant la compareixença personal de la persona afectada. La raó d'aquest règim diferent entre entitats privades i públiques obeeix al fet que, quan s'actua davant les administracions públiques, el RLOPD està condicionat per l'article 32 de la LRJPA, pel principi de jerarquia normativa, i per això s'ha limitat a transcriure aquest precepte.

En cas que la sol•licitud d'exercici dels drets ARCO la faci una persona diferent a l'afectada o no s'acrediti la representació, l'article 23.3 del RLOPD disposa que "es denegarà". Cal entendre que això serà així si és una persona diferent a l'afectada qui exerceix el dret i ho fa en el seu propi nom i no en el de l'afectada, però si el problema és que no acredita correctament la representació, aleshores s'hauria de requerir l'esmena del defecte, en consonància amb l'article 25.3 del RLOPD, i en el cas d'exercici davant les administracions públiques encara amb més raó per l'aplicació dels articles 32.4 i 71 de la LRJPA.

Continuant amb la representació i deixant un moment l'àmbit general de la legislació de protecció de dades, cal fer notar que en l'àmbit sectorial específic de dades personals de la salut, i concretament pel que fa al dret d'accés a la història clínica, tant l'article 13 de la Llei 21/2000 (catalana) com l'article 18.2 de la Llei 48/2002 (estatal), permeten la representació sempre que "estigui degudament acreditada".

Sobre els menors, l'article 23.2.b) del RLOPD, que abans s'ha avançat en tractar el cas de representació forçosa, sembla equiparar la minoria d'edat amb la incapacitat i exigeix que l'acció la formuli el representant legal. No s'ha inclòs aquí expressament, o almenys no de forma clara, la possibilitat que el menor actuï per si mateix quan ja té els 14 anys, tal com s'ha fet en regular la prestació del consentiment a l'article 13 del RLOPD. De tota manera, sembla que el més lògic seria que si als menors però majors de 14 anys se'ls permet prestar el consentiment per al tractament de les seves dades, també se'ls hauria de permetre, en principi, l'exercici dels drets ARCO, i fins i tot el procediment administratiu de tutela que es pogués tramitar després davant l'autoritat de control, en cas d'una eventual denegació del dret, ja que l'article 30 de la LRJPA admet la capacitat d'actuar dels menors davant les administracions públiques si així ho ha previst la normativa aplicable.

Una altra conseqüència del caràcter personalíssim dels drets ARCO és que no els poden exercir els hereus de la persona finada, ja que extingida la persona, s'extingeix el dret. No obstant això, l'article 2.4 del RLOPD, després d'advertir que la legislació de protecció de dades no és d'aplicació a les persones mortes, preveu que les persones vinculades al mort, ja sigui per raons familiars o anàlogues, es poden dirigir als responsables dels fitxers o tractaments que continguin dades de la persona morta amb la finalitat de notificar l'òbit, aportant l'acreditació suficient, i sol·licitar, quan escaigui, la cancel·lació de les dades. Ara bé, més que de l'exercici d'un dret ARCO, concretament el de cancel·lació, aquesta regulació seria una manifestació del principi de qualitat de les dades, en allò referent a la necessitat que les dades siguin exactes i posades al dia, de manera que responguin amb veracitat a la situació actual (article 8.5 del RLOPD).

Exercici dels drets davant l'encarregat del tractament

L'article 26 del RLOPD introdueix la possibilitat d'exercir els drets ARCO davant l'encarregat del tractament, el qual traslladarà la sol·licitud al responsable a fi que sigui ell qui faci efectiu el dret, o bé l'atendrà ell mateix si així s'ha previst al contracte corresponent.

Un exemple d'exercici dels drets ARCO davant l'encarregat del tractament seria el cas d'un despatx d'advocats que envia reclamacions de deutes a clients de les empreses creditores, supòsit en què l'empresa és la responsable del fitxer i el despatx d'advocats, l'encarregat de tractament. En aquest cas, la persona afectada podrà, per exemple, exercir el dret d'accés davant el despatx d'advocats, com a encarregat del tractament, el qual l'haurà traslladar al responsable del fiter per tal que el faci efectiu, o bé l'haurà de fer efectiu el mateix despatx d'advocats per encàrrec del responsable, si així s'havia previst en el contracte d'encàrrec de tractament.

Dret d'accés

Contingut

Des d'una perspectiva supraestatal, el dret d'accés està regulat a l'article 8 del Conveni 108, del Consell d'Europa, i també a l'article 12 de la Directiva 95/46. El dret d'accés suposa en essència el dret de la persona afectada a conèixer si les seves dades es tracten, amb quina finalitat són tractades, així com a saber l'origen i les comunicacions a tercers efectuades i a obtenir informació del responsable de les dades. El dret d'accés està relacionat amb el principi de qualitat de les dades, ja que l'article 4.6 de la LOPD, quan regula aquest principi disposa que les dades han de ser emmagatzemades ("tractades", diu l'article 8.7 del RLOPD) de manera que permetin l'exercici del dret d'accés.

Els articles 15.1 de la LOPD i 27 del RLOPD fan referència al contingut del dret d'accés i determinen que consisteix en el dret de la persona afectada a saber:

1. si s'estan tractant les seves dades personals,
2. amb quina finalitat,
3. la informació sobre l'origen de les dades, i
4. les comunicacions o cessions previstes (d'on vénen i on van).

Per tal d'evitar que un abús d'aquest dret pogués generar disfuncions o esforços desproporcionats en el responsable del fitxer, l'article 27.2.2 del RLOPD permet que, quan hi hagi raons d'especial complexitat que ho justifiquin, el responsable del fitxer podrà requerir a la persona afectada per tal que especifiqui respecte de quins fitxers vol exercir el dret d'accés, però a aquest efecte caldrà facilitar-li una relació de tots els fitxers. La interpretació d'aquest precepte pot donar lloc a problemes, com tots els que contenen conceptes jurídics indeterminats. Quan som davant de "raons d'especial complexitat que justifiquin exigir la concreció"? Com tota limitació a un dret, i encara més pel seu caràcter de dret fonamental, s'hauria d'aplicar de forma restrictiva i amb molta prudència.

En el cas de fitxers i tractaments de les administracions públiques, la coincidència de dos drets denominats "d'accés" (accés a dades personals en la LOPD i accés a arxius i registres en la LRJPA) ha portat l'article 27.3 del RLOPD a precisar que el dret d'accés de la LOPD és independent del dret d'accés a arxius i registres de la LRJPA o d'altres lleis sectorials. Certament, aquest "altre dret d'accés" no es refereix només a l'accés a informació personal de la persona afectada, sinó que es refereix a l'accés a informació personal de qualsevol tipus, ja sigui referent a la persona interessada o a d'altres persones, i en moltes ocasions referent a procediments de l'administració pública en què no hi ha una persona física interessada. Això no impedeix, però, que en ocasions, en concret quan l'accés pretès es refereix a dades de la persona afectada i no a

d'altres, ens trobem amb dos camins alternatius que permetrien arribar al mateix resultat: l'accés a la informació sobre la persona afectada.

Retornant al dret d'accés de la LOPD, aquesta llei permet a la persona afectada saber, entre d'altres aspectes, el tractament que es fa de les seves dades, ara bé no recull el dret a saber qui són les persones que fan el tractament, és a dir la identitat de les persones empleades o funcionàries concretes que les tracten. Això s'ha plantejat en casos en què la persona afectada volia saber la identitat del funcionari o la funcionària que tramitava el seu expedient tributari, i sempre s'ha denegat el dret a conèixer-la.

Exercici del dret d'accés

La regulació de l'exercici del dret està recollida a l'article 15 de la LOPD i, amb més detall, a l'article 28 del RLOPD. De l'aplicació conjunta d'ambdós preceptes es desprèn que, quan exerceix el dret d'accés, la persona afectada pot optar entre diferents modalitats:

1. visualització en pantalla.
2. correu certificat o sense certificar. La possibilitat que la persona afectada demani l'opció de correu no certificat dificultaria, després, al responsable del fitxer, complir amb l'article 25.5 del RLOPD, que l'obliga a poder acreditar que s'ha donat resposta i a conservar-ne l'acreditació (avís de recepció per correu certificat).
3. Telecòpia (fax)
4. Correu electrònic o altres sistemes de comunicació electrònica.
5. Qualsevol altre sistema adequat al fitxer o tractament.

L'article 28.2 del RLOPD preveu que aquests diferents sistemes de consulta es poden restringir per la singularitat del fitxer o tractament, sempre que s'ofereixi a la persona afectada un sistema alternatiu gratuït i s'asseguri la comunicació escrita si la persona afectada ho exigeix.

L'article 28.3 del RLOPD afegeix que, en fer-se efectiu l'accés, el responsable ha de complir amb les mesures de seguretat exigibles i, si no ho fa, se li podrien imputar les responsabilitats corresponents. A continuació, el mateix precepte fa alguna precisió concreta i detalla que si el responsable ofereix a la persona afectada un sistema per fer efectiu l'accés i la persona afectada el rebutja, el responsable no haurà de respondre pels possibles riscos. Per exemple, si s'ofereix la visualització en pantalla, però la persona afectada prefereix telecòpia o correu sense certificar perquè mai no és al seu domicili particular i no vol desplaçar-se a correus, si la informació arriba a mans d'algú diferent, no podrà queixar-se. En una línia semblant, el precepte també preveu que si la persona afectada exigeix un sistema que comporta un cost desproporcionat per al responsable del fitxer o tractament, aquest podrà exigir a la persona afectada que assumeixi el cost. Seria el cas, per exemple, en què l'efectivitat del dret d'accés exigís manegar molta documentació i que, enlloc de rebre-la en format electrònic, la persona afectada la volgués rebre en paper i amb correu certificat. Novament, però, ens trobem amb el problema dels conceptes jurídics indeterminats, en aquest cas el de "cost desproporcionat".

Atorgament de l'accés

L'article 29 del RLOPD disposa que s'ha de de donar resposta a la sol•licitud d'accés en el termini màxim d'un mes, encara que sigui per comunicar que no consten dades de la persona afectada. Si s'estima la sol•licitud d'accés, però amb la resposta no s'acompanya la documentació i la informació demanada, és a dir, si no es tramet amb la resposta la informació pretesa, l'accés es farà efectiu dins dels 10 dies hàbils següents.

En coherència amb la definició del contingut del dret d'accés que fan els articles 15 de la LOPD i 27 del RLOPD, el 29.3 del RLOPD recorda novament que en la informació proporcionada a la persona afectada hi han de constar les dades de base de la persona, les resultants de qualsevol tractament informàtic, així com l'origen, els cessionaris previstos i els usos i les finalitats. Tota

aquesta informació s'ha de facilitar, òbviament, de forma legible i intel•ligible, i sense utilitzar claus o codis que en dificultin la interpretació.

Denegació de l'accés

La legislació de protecció de dades preveu dos supòsits específics de denegació del dret accés. Un primer cas en què la denegació obeeix a una qüestió temporal i un segon grup de casos referits a l'existència d'unes raons de fons:

1. Quan la mateixa persona afectada ja l'hagi exercit en els 12 mesos anteriors, òbviament davant el mateix responsable del fitxer i sobre les mateixes dades (excepció prevista per la mateixa LOPD en l'article 15.3 i recollida també a l'article 30.1 del RLOPD). En aquest supòsit existeix una presumpció d'abús del dret que permet denegar l'accés, però aquesta presumpció la pot desvirtuar la persona afectada si acredita la concurrència d'un "interès legítim" que justifiqui accedir-hi novament abans que transcorri el termini esmentat.
2. Quan una llei o norma comunitària d'aplicació directa preveu la denegació de l'accés o impedeix al responsable revelar a la persona afectada el tractament de les dades a les quals es refereix l'accés. Al marge del fet que els articles 23 de la LOPD i 25 del RLOPD preveuen expressament la possibilitat de modular els drets ARCO per raons de seguretat pública, i per tant també el dret d'accés, l'article 30.2 del RLOPD es refereix a excepcions previstes per lleis sectorials. Podria ser el cas de prevenció de blanqueig de capitals, en què la llei que ho regula disposa que l'entitat financera no hauria de comunicar a la persona afectada el tractament que s'està fent amb les seves dades. D'acord amb la pròpia legislació de protecció de dades de caràcter personal, també procedeix la denegació quan la sol·licitud d'accés l'ha efectuat una persona diferent a la persona afectada, atès el caràcter personalíssim del dret. Aquest seria el cas, per exemple, d'una persona que exercís el dret d'accés en relació amb dades personals del seu ex cònjuge.

Drets de rectificació i de cancel·lació

Contingut

Els drets de rectificació i cancel·lació tenen una vinculació evident amb el principi de qualitat de les dades, que com ja s'ha dit pretén evitar que les dades siguin inexactes o incompletes, o bé que es tractin dades que legalment haurien d'estar cancel·lades. Així doncs, amb el reconeixement d'aquest dret a la rectificació o la cancel·lació es pretén assegurar el principi de qualitat de les dades.

L'article 16 de la LOPD es refereix a alguns aspectes relatius als drets de rectificació i cancel·lació, però no en defineix el significat, cosa que sí que fa el RLOPD. Així, l'article 31.1 del RLOPD defineix el dret de rectificació com el dret de la persona afectada que es modifiquin les dades que siguin inexactes o incompletes.

Pel que fa al dret de cancel•lació, l'article 31.2 del RLOPD el defineix com el dret que se suprimeixin les dades que resultin inadequades o excessives, sense perjudici del deure de bloqueig. Aquest redactat inverteix la fórmula emprada per l'article 16.3 de la LOPD, el qual disposa que la cancel•lació dóna lloc al bloqueig, i que les dades només s'han de conservar a disposició de les autoritats que les necessiten per atendre les responsabilitats corresponents durant el termini en què es puguin exigir. Afegeix aquest precepte que, un cop transcorregut aquest termini, les dades s'han de suprimir. En tot cas, el significat és el mateix, perquè el dret de cancel•lació no implica automàticament la destrucció de les dades, sinó que això es pot fer únicament quan ja no siguin necessàries i s'hagin satisfet les obligacions corresponents. Quan això s'esdivingui, aleshores sí que existeix el deure de cancel•lar.

L'article 31.2 del RLOPD fa, al segon paràgraf, una remissió a la LOPD, en relació amb el supòsit que la persona afectada invoqui el dret de cancel•lació per revocar el consentiment prestat prèviament. Aquesta remissió s'ha d'entendre efectuada a l'article 6.3 de la LOPD, en la qual s'admet aquesta revocació del consentiment prestat prèviament, sempre que hi hagi una causa justificada i que aquesta revocació no tingui efectes retroactius.

Exercici dels drets de rectificació i cancel•lació

En relació amb la sol·licitud d'exercici del dret de rectificació, l'article 32.1 del RLOPD disposa que cal indicar a quines dades es refereix i la correcció que se n'ha de fer, i que ha d'anar acompanyada de la documentació justificativa de la rectificació que se sol·licita.

Respecte a les sol·licituds d'ambdós drets, els articles 16.1 de la LOPD i 32.2 del RLOPD disposen que s'han de resoldre en 10 dies hàbils i, de la mateixa manera que succeeix en el dret d'accés, si no es disposa de dades s'ha d'informar d'aquesta circumstància la persona afectada en el mateix termini. En relació amb el termini, la pràctica administrativa està demostrant que és un termini molt curt i que hi ha dificultats, en ocasions, per poder-lo respectar.

L'article 16.4 de la LOPD i el 32.3 del RLOPD disposen que, si les dades rectificades o cancel•lades s'haguessin cedit prèviament a un tercer, una vegada efectuada la rectificació o cancel·lació el responsable l'ha de comunicar, en el termini de 10 dies, al cessionari, per tal que en un nou termini de 10 dies més rectifiqui o cancel·li les seves dades. Aquesta última rectificació o cancel•lació no requereix ser comunicada a la persona afectada.

Amb la resposta a l'exercici del dret de cancel·lació, s'haurien de bloquejar les dades, tret que aquestes s'haguessin obtingut de manera fraudulenta, deslleial o il·lícita, ja que en aquest cas l'actuació procedent seria la supressió sense bloqueig.

També, en clara connexió amb el principi de qualitat de les dades de l'article 4 de la LOPD i, concretament, amb l'article 4.5 de la LOPD en el qual s'estableix el deure de cancel·lar les dades personals quan hagin deixat de ser necessàries o pertinents per a la finalitat per a la qual havien estat recollides o registrades, l'article 16.5 de la LOPD preveu la conservació de les dades durant els terminis que preveuen les disposicions aplicables o, si s'escau, les relacions contractuals entre l'entitat responsable del tractament i la persona afectada.

Denegació dels drets de rectificació i cancel•lació

En abordar en general el conjunt dels drets ARCO, ja s'ha dit que l'article 25.7 del RLOPD permet la seva *modulació* per raons de seguretat pública, en els casos i amb l'abast previst a les lleis. Ja hem vist que la mateixa LOPD preveu, a l'article 23, excepcions a l'exercici dels drets ARCO en casos de perill per a la defensa de l'estat o seguretat pública, o en casos concrets en l'àmbit de la hisenda pública.

En particular, en relació amb els drets de rectificació i cancel·lació que ara estudiem, també hem avançat que l'article 25.8 del RLOPD admet la possibilitat que se segueixi el previst a les normes sectorials, com en els casos de determinats registres.

La denegació dels drets de rectificació i cancel·lació amb caràcter general està regulada a l'article 33 del RLOPD. En primer terme, l'article 33.1 del RLOPD disposa que la petició de cancel•lació (no de rectificació) es pot denegar quan les dades s'han de conservar durant els terminis previstos a l'ordenament o en els casos de relacions contractuals entre el responsable del fitxer i la persona afectada que van justificar el tractament. Aquesta denegació que preveu el RLOPD seria possible, doncs, només mentre existeixin obligacions o responsabilitats pendents, però no un cop liquidades o extingides aquestes.

L'article 33.2 del RLOPD preveu la denegació de rectificació i cancel•lació en els casos previstos en una llei o norma comunitària, denegació idèntica a la prevista per al dret d'accés a l'article 30.2 del RLOPD.

Per acabar, l'article 33.3 del RLOPD obliga, per als casos de denegació del dret, a informar la persona afectada del seu dret a demanar la tutela a l'autoritat de control competent, de la mateixa manera que succeeix amb la resta de drets ARCO quan el responsable del fitxer o tractament no els fa efectius.

Cal recordar novament, perquè ja s'ha avançat anteriorment en parlar del caràcter personalíssim dels drets ARCO, que quan el RLOPD defineix el seu àmbit d'aplicació preveu, a l'article 2.4, que no és d'aplicació a les dades de les persones finades, si bé determina que les persones que hi estan vinculades, si acrediten la mort, poden demanar la cancel•lació. Encara que s'usa el mot cancel•lació, no s'ha ubicat aquest supòsit al capítol dels drets ARCO, perquè més que considerar-se com un exercici del dret de cancel•lació per part dels familiars, la finalitat és facilitar el principi de qualitat, és a dir, garantir que les dades s'ajustin a la realitat i estiguin actualitzades. Això deriva del caràcter personalíssim dels drets ARCO, d'acord amb el qual una vegada extingida la persona, s'extingeix el dret.

Dret d'oposició

Contingut

Ni a la LORTAD de 1992, ni al Reglament que la desenvolupava no es regulava el dret d'oposició expressament com a tal, que sí que es va preveure a la LOPD -a l'article 6.4, entre d'altres- tot i que sense definir-lo ni sistematitzar-lo. En canvi, el RLOPD sí que l'ha definit i ha dotat aquest dret d'una regulació completa.

El dret d'oposició el podem definir, en essència, com el dret de la persona afectada al fet que no es dugui a terme el tractament de les seves dades personals, sempre que hi hagi una causa justificada. Segons la LOPD, es podrà exercir aquest dret en relació amb tractaments en què no calia el consentiment de la persona afectada, quan concorri un motiu legítim i fonamentat referit a una situació personal concreta que justifiqui l'oposició al tractament, i sempre que la llei no disposi el contrari.

Aquest és el contingut essencial del dret d'oposició, el qual ja estava previst a l'article 6.4 de la LOPD, i és el que apareix en primer lloc a l'article 34 del RLOPD, concretament a la lletra *a*. A continuació, aquest Reglament afegeix dos supòsits més en què la persona afectada també pot oposar-se al tractament de les seves dades personals:

b) Quan es tracti de fitxers d'activitats de publicitat i prospecció comercial, en els termes que estableix l'article 51 del RLOPD, el qual regula aquest dret d'oposició per a aquest cas concret.

c) Quan el tractament tingui per finalitat l'adopció d'una decisió referida a la persona afectada basada únicament en un tractament automatitzat de les seves dades, supòsit desenvolupat a l'article 36 del RLOPD i que veurem més endavant.

Exercici del dret d'oposició

El dret d'oposició s'exerceix davant el responsable del tractament i, en cas que la persona afectada invoqui un motiu legítim i fonamentat per oposar-se a un tractament per al qual no calia consentiment (és a dir el supòsit de la lletra *a*), l'haurà de justificar en la sol•licitud.

La sol•licitud s'ha de contestar en 10 dies, i en la resposta hi ha de constar l'acceptació de l'exclusió del tractament al qual s'ha oposat la persona afectada o bé la denegació motivada de la sol•licitud. La resposta s'ha d'efectuar en qualsevol cas, fins i tot en cas que no hi constin dades de la persona afectada.

Si transcorre el termini indicat i la persona afectada no rep cap resposta o bé si la resposta és desestimatòria, es podrà interposar reclamació de tutela del dret en els termes previstos a l'article 18 de la LOPD.

Dret d'impugnació de valoracions

Es coneix com a dret d'impugnació de valoracions el dret d'oposar-se a les decisions basades únicament en un tractament automatitzat de dades. Aquest dret ja s'havia previst a l'article 12 de la LORTAD i està regulat a l'article 13 de la LOPD, encara que és al RLOPD, concretament als articles 34, 35 i 36.1, on s'ha sistematitzat més clarament com una manifestació del dret d'oposició, .

L'article 36 del RLOPD es dedica exclusivament a aquest dret i el configura com el dret de la persona a no veure's sotmesa a decisions amb efectes jurídics basades únicament en un tractament automatitzat destinat a avaluar determinats aspectes de la seva personalitat, com ara el seu rendiment laboral, el crèdit, la fiabilitat o la conducta.

Aquest dret es podria aplicar, per exemple, en el cas d'una valoració automatitzada efectuada per un programa informàtic que avalués la persona usuària segons diferents paràmetres vinculats a l'ús que fa de l'ordinador.

El mateix article 36 del RLOPD, però, admet com a lícites aquestes valoracions automatitzades en dos casos:

1. Quan s'hagi adoptat en el marc de l'execució d'un contracte a petició de la persona interessada, sempre que tingui possibilitat de fer al•legacions.
2. Quan estigui autoritzada per una norma amb rang de llei que estableixi mesures per garantir l'interès legítim de la persona afectada.

Procediment de tutela de drets

Els articles 18 de la LOPD i 7 de la Llei 5/2002, de l'APDCAT, que té com a títol *Tutela dels drets*, disposen que la persona a qui es denegui, totalment o parcialment, l'exercici dels drets ARCO pot posar aquest fet en coneixement de l'autoritat de control competent, a la qual correspon assegurar la procedència o improcedència de la denegació. Així doncs, es tracta d'un procediment que sempre s'inicia a instància de la persona afectada, mitjançant la reclamació corresponent.

Sobre aquest procediment de tutela dels drets ARCO, la LOPD només afegeix que la resolució del procediment s'ha de dictar en el termini de sis mesos (la Llei 5/2002, de l'APDCAT, redueix aquest termini a tres mesos) i que contra la resolució que dicti l'autoritat de control es podrà interposar recurs contenciós administratiu.

Com és natural, la regulació d'aquest procediment de tutela dels drets ARCO s'ha previst al RLOPD i l'analitzarem en els apartats següents.

Reclamació en cas de silenci administratiu

En relació amb l'exercici dels drets ARCO davant el responsable del fitxer o tractament, el RLOPD ha previst de forma implícita una mena de silenci desestimatori, en disposar que si en el termini que correspongui en cada dret no s'ha donat resposta, és a dir no s'ha resolt i notificat a la persona interessada, aquesta podrà formular reclamació davant l'autoritat de control.

Aquest sistema no ofereix cap problema en el cas dels fitxers d'entitats privades, però en el cas que la sol•licitud s'hagi exercit davant les administracions públiques pot sorgir el dubte de si aquest règim atempta contra el règim del silenci de la LRJPA, que preveu amb caràcter general el silenci estimatori per a totes les sol•licituds i que assenyala que només es pot invertir a silenci desestimatori si una norma amb rang de llei o una norma comunitària ho preveuen expressament, però no un reglament, com seria el cas del RLOPD.

El cas és que la LOPD, concretament l'article 18 que regula la tutela dels drets ARCO, i encara que no ho digui expressament, sembla emparar aquest silenci desestimatori quan disposa que les

actuacions contràries a la pròpia LOPD poden ser objecte de reclamació, i es podria entendre com una actuació "contrària a la LOPD" el fet de no contestar en el termini previst per aquesta Llei.

Reclamació en cas de denegació expressa dels drets ARCO

Quan es denega de forma expressa, ja sigui totalment o parcialment, la sol·licitud del dret d'accés, rectificació, cancel·lació o oposició, el RLOPD imposa al responsable del fitxer o tractament el deure d'informar la persona afectada del seu dret a demanar la tutela de les autoritats independents.

El RLOPD recorda l'obligació d'incloure, en la denegació, allò que en l'àmbit dels procediments administratius tramitats per les administradions es coneix com *peu de recurs*, en el qual s'informa la persona interessada de les accions que té al seu abast, del termini per dur-les a terme i davant de qui s'han de formular. Hi ha en aquest punt, però, una diferència que cal subratllar, i és que per exercir la reclamació davant l'autoritat independent no existeix un termini (cal, això sí, que hagi transcorregut el termini per contestar la sol•licitud inicial, ja sigui 1 mes en el dret d'accés o 10 dies en la resta), de manera que es podria presentar la reclamació de forma indefinida, en tractar-se d'un dret que no prescriu i que només s'extingeix quan s'extingeix la persona afectada, sense que es pugui transmetre el dret als hereus atès el seu caràcter personalíssim.

Inici del procediment de tutela dels drets ARCO

Com ja s'ha dit, quan la sol•licitud dels drets ARCO es denega totalment o parcialment, o el responsable del fitxer no contesta dins del termini establert, la persona afectada pot formular reclamació davant l'autoritat independent corresponent. Aquesta reclamació és la que inicia el procediment regulat als articles que van del 117 al 119 del RLOPD. En tractar-se d'un procediment administratiu iniciat a instància de part, la reclamació o sol·licitud de tutela ha de reunir els requisits que l'article 70 exigeix per a les sol·licituds d'inici de procediments.

A més, d'acord amb l'article 117.1 del RLOPD, la persona afectada haurà d'expressar amb claredat el contingut de la seva reclamació i els preceptes de la LOPD que considera vulnerats.

Instrucció del procediment

D'acord amb l'article 117.2 del RLOPD, quan l'autoritat competent rep la reclamació, l'ha de traslladar al responsable del fitxer per tal que formuli al•legacions en el termini de 15 dies hàbils.

L'article 117.3 del RLOPD afegeix que una vegada rebudes aquestes al•legacions o transcorregut el termini de 15 dies, es podrien dur a terme els actes d'instrucció necessaris, que podrien comprendre la petició d'informes, la pràctica de proves i també l'audiència de la persona afectada i novament del responsable del fitxer, per tal de, finalment, dictar la resolució.

De tots aquests tràmits previstos a l'article 117 del RLOPD, el que és imprescindible és el primer trasllat de la reclamació al responsable del fitxer per tal que formuli al•legacions, però en molts casos serien innecessaris la resta d'actes d'instrucció, de manera que no caldria practicar proves ni demanar informes. Fins i tot es podria prescindir del segon tràmit d'audiència a la persona afectada i novament al responsable del fitxer i dictar directament resolució, si en aquesta no s'haguessin de tenir en compte altres fets i al•legacions que les adduïdes per les parts interessades en la reclamació i primera audiència al responsable fitxer, tal com autoritza l'article 84.4 de la LRJPA.

Durada del procediment i efectes del silenci

L'article 18.3 LOPD disposa que el termini màxim per tramitar el procediment de tutela de drets és de sis mesos i que en cas que no es resolgui i notifiqui en aquest termini, la persona afectada pot entendre estimada la seva reclamació per silenci estimatori, efecte que té exactament el mateix

valor jurídic que una estimació expressa, de manera que el responsable del fitxer podria impugnar aquest silenci estimatori en cas de desacord.

Cal subratllar novament que en el cas de procediments tramitats per l'APDCAT el termini màxim d'aquest procediment és de tres mesos, perquè així ho imposa l'article 7.2 de la Llei 5/2002, de l'APDCAT. Aquesta circumstància justifica encara més la necessitat de simplificar al màxim els actes d'instrucció del procediment i per això normalment es prescindeix de la segona audiència a la persona reclamant i al responsable del fitxer, tret que això sigui necessari perquè en la resolució s'haguessin de tenir en compte fets no coneguts per les persones interessades.

Execució de la resolució

La resolució del procediment la dicta el director o la directora de l'autoritat de control competent. Si la resolució és estimatòria, es requerirà el responsable del fitxer o tractament per tal que en 10 dies faci efectiu l'exercici dels drets ARCO objecte de tutela, i s'haurà de donar compte per escrit d'aquest compliment a l'autoritat de control en un termini de 10 dies més.

Si el responsable incompleix amb aquesta obligació de donar compte a l'autoritat que ha executat la resolució, podria incórrer en la infracció greu prevista a l'article 44.3.i) de la LOPD per no aportar a l'autoritat de control la documentació requerida, la qual cosa podria donar lloc a la incoació d'un procediment sancionador.

Dret a indemnització

L'article 19 de la LOPD reconeix el dret d'indemnització d'aquelles persones que, com a conseqüència de vulneracions de la LOPD comeses pel responsable o encarregat del tractament, pateixin algun dany o lesió en els seus béns o drets.

En cas de fitxers de titularitat pública, l'article 19.2 de la LOPD preveu que la indemnització s'ha d'exigir conforme a la legislació reguladora del règim de responsabilitat patrimonial de les administracions públiques, que trobem a l'article 139 i als articles següents de la LRJPA. Sobre això, l'article 139 de la LRJPA recull amb caràcter general aquest dret d'indemnització establert a l'article 106.2 de la Constitució Espanyola, reconegut per als casos de lesió que pateixin els ciutadans com a conseqüència del funcionament normal o anormal dels serveis públics, tret dels casos de força major. Com a requisits bàsics per a la procedència de la indemnització, s'exigeix que el dany al·legat sigui efectiu, avaluable econòmicament i individualitzat. En cas que es denegui la indemnització en la via administrativa, cal recórrer a la via de la jurisdicció contenciosa administrativa.

En cas de fitxers de titularitat privada, l'article 19.3 de la LOPD disposa que l'acció s'exercirà davant els òrgans de la jurisdicció ordinària. En la via civil també es podria tenir la cobertura de la Llei orgànica 1/1982, de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge. Fins i tot aquesta acció civil també es podria fonamentar en l'article 1902 del Codi civil.

Unitat 5: Les autoritats de protecció de dades

Règim general de les autoritats de protecció de dades

La legislació de protecció de dades ha creat unes **institucions específiques** a les quals ha encomanat la funció de **vetllar pel respecte del dret a la protecció de dades personals**. Són les agències o autoritats de protecció de dades

Aquestes institucions són **entitats de dret públic** amb plena capacitat jurídica d'obrar i que actuen amb plena independència de la resta de poders públics. És a dir, no estan subjectes a cap mandat imperatiu.

De fet, podem afirmar que la seva característica principal és la **independència** davant la resta d'administracions públiques i entitats privades a les quals ha de controlar en allò que es refereix al tractament de dades personals.

La mateixa **Directiva 95/46/CE** estableix la necessitat que existeixin i així ho indica en l'article 28, el qual disposa que els estats membres han d'establir que una o més autoritats públiques s'encarreguin de vigilar l'aplicació en el seu territori de les disposicions en matèria de protecció de dades. Aquesta mateixa Directiva recorda que aquestes autoritats han d'exercir les seves funcions amb total independència.

La **LOPD** transposa, en el Títol VI, l'article 28 de la Directiva, i la **Llei 5/2002, de 19 d'abril,** de creació de l'Agència Catalana de Protecció de Dades, estableix també un règim jurídic similar.

La regulació de l'Agència Catalana de Protecció de Dades es veurà en detall a continuació, en el punt 3 d'aquesta unitat.

L'Agència Espanyola de Protecció de Dades

Respecte de l'Agència Espanyola de Protecció de Dades (en endavant, AEPD), només en farem una breu referència. Aquesta entitat és l'autoritat de protecció de dades encarregada de vetllar pel dret a la protecció de dades en aquelles comunitats autònomes on no s'ha creat una autoritat específica. Tot i que a Catalunya es va crear l'Agència Catalana de Protecció de Dades, l'AEPD seria competent respecte d'aquelles entitats privades que no s'inclouen en l'article 156 de l'Estatut d'Autonomia de Catalunya, qüestió que es veurà en detall en el punt següent d'aquesta unitat.

L'AEPD és un ens de dret públic, amb personalitat jurídica pròpia i plena capacitat pública i privada, que actua amb plena independència de les administracions públiques en l'exercici de les seves funcions.

L'AEPD està formada pels òrgans següents:

- Direcció
- Consell Consultiu
- Registre General de Protecció de Dades

La direcció

L'AEPD està representada i dirigida per un director o una directora que es nomena, d'entre els membres del Consell Consultiu, per un període de quatre anys, exerceix les funcions amb plena independència i objectivitat, i no està subjecte a cap instrucció en l'exercici de les seves funcions.

Les causes de cessament estan fixades i són:

- incompliment greu de les seves obligacions,
- incapacitat sobrevinguda per a l'exercici de la seva funció,
- incompatibilitat, i
- condemna per delicte dolós.

Les funcions de l'Agència estan regulades a l'article 37 de la LOPD.

El Consell Consultiu

És l'òrgan que assessora el director o la directora de l'Agència. A l'article 38 de la LOPD es regula la seva composició, la qual intenta establir una representació plural.

Els seus informes no són preceptius, excepte en el cas de destitució del director o la directora i, en aquest cas, l'informe s'adreça al Ministeri de Justícia.

El Registre General de Protecció de Dades (RGPD)

És un òrgan integrat a l'Agència Espanyola de Protecció de Dades que té com a missió vetllar per la publicitat dels fitxers i tractaments de dades amb la finalitat de garantir el dret a la protecció de dades personals, i en concret, facilitar l'exercici dels drets d'accés, rectificació, cancel·lació i oposició.

L'Agència Catalana de Protecció de Dades

La LOPD estableix que les funcions que porta a terme l'Agència Espanyola de Protecció de Dades, excepte les esmentades a l'article 37 de la LOPD en els apartats j), k) i l), i en els apartats f) i g) pel que fa a les transferències internacionals de dades, i als articles 46 i 49, han de ser exercides per les autoritats de control de cada Comunitat Autònoma dins del marc competencial que els correspongui.

A Catalunya correspon exercir-les a l'Agència Catalana de Protecció de Dades creada per la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades.

Funcions que no porta a terme l'Agència Catalana de Protecció de Dades

Article 37 de la LOPD:

j) Vetllar per la publicitat de l'existència dels fitxers de dades amb caràcter personal; a

aquest efecte, ha de publicar periòdicament una relació dels fitxers esmentats amb la informació addicional que el director de l'Agència determini.

k) Redactar una memòria anual i remetre-la al Ministeri de Justícia.

l) Exercir el control i adoptar les autoritzacions que siguin procedents en relació amb els moviments internacionals de dades, així com exercir les funcions de cooperació internacional en matèria de protecció de dades personals.

Article 37 de la LOPD, en allò que afecta a les transferències internacionals:

f) Requerir als responsables i als encarregats dels tractaments, amb l'audiència prèvia d'aquests, l'adopció de les mesures necessàries per a l'adequació del tractament de dades a les disposicions d'aquesta Llei i, si escau, ordenar la cessació dels tractaments i la cancel·lació dels fitxers, quan no s'ajustin a les seves disposicions.

g) Exercir la potestat sancionadora en els termes que preveu el títol VII d'aquesta Llei.

Naturalesa jurídica

L'Agència Catalana de Protecció de Dades (en endavant, apdcat) té per objecte vetllar pel respecte dels drets fonamentals i les llibertats públiques dels ciutadans en tot allò que concerneix les operacions fetes mitjançant processos automatitzats o manuals de dades personals, dins l'àmbit d'actuació que legalment s'estableixi.

Com ja veiem en relació amb l'AEPD, l'apdcat és una institució de dret públic, amb personalitat jurídica pròpia i plena capacitat d'obrar per al compliment dels seus fins, que actua amb objectivitat i plena independència de les administracions públiques en l'exercici de les seves funcions.

Àmbit d'actuació

Des de l'entrada en vigor de l'Estatut d'Autonomia de Catalunya, l'àmbit d'actuació de l'apdcat apareix configurat a l'article 156 d'aquesta norma, segons el qual:

Correspon a la Generalitat la competència executiva en matèria de protecció de dades de caràcter personal que, respectant les garanties dels drets fonamentals en aquesta matèria, inclou en tot cas:

1. La inscripció i el control dels fitxers o els tractaments de dades de caràcter personal creats o gestionats per les institucions públiques de Catalunya, l'Administració de la Generalitat, les administracions locals de Catalunya, les entitats autònomes i les altres entitats de dret públic o privat que depenen de les administracions autonòmica o locals o que presten serveis o acompleixen activitats per compte propi per mitjà de qualsevol forma de gestió directa o indirecta, i les universitats que integren el sistema universitari català.
2. La inscripció i el control dels fitxers o els tractaments de dades de caràcter personal privats creats o gestionats per persones físiques o jurídiques per a l'exercici de les funcions públiques amb relació a matèries que són competència de la Generalitat o dels ens locals de Catalunya, si el tractament s'efectua a Catalunya.
3. La inscripció i el control dels fitxers i els tractaments de dades que creïn o gestionin les corporacions de dret públic que exerceixin llurs funcions exclusivament en l'àmbit territorial de Catalunya.
4. La constitució d'una autoritat independent, designada pel Parlament, que vetlli per garantir el dret a la protecció de les dades personals en l'àmbit de les competències de la Generalitat.

Competències i funcions

Les competències de l'apdcat es poden classificar en competències de registre, control, inspecció, sanció i resolució, així com d'adopció de propostes i instruccions.

Les funcions que porta a terme l'apdcat són:

1. Vetllar pel compliment de la legislació vigent sobre protecció de dades de caràcter personal i controlar-ne l'aplicació, especialment en allò que fa referència als drets d'informació, accés, rectificació, cancel·lació i oposició.
2. Vetllar pel compliment de les disposicions que la Llei d'estadística de Catalunya estableix respecte a la recollida de dades estadístiques i al secret estadístic. L'Agència, dins del seu àmbit de competències, pot adoptar instruccions i resolucions adreçades als òrgans administratius i pot sol·licitar la col·laboració de l'Institut d'Estadística de Catalunya, quan s'escaigui.
3. Dictar les instruccions necessàries per adequar els tractaments de dades personals als principis de la legislació vigent en matèria de protecció de dades de caràcter personal.
4. Requerir als responsables i als encarregats del tractament l'adopció de les mesures necessàries per a l'adequació del tractament de dades personals objecte d'investigació a la legislació vigent en matèria de protecció de dades de caràcter personal i, si escau, ordenar el cessament dels tractaments i la cancel·lació dels fitxers.
5. Proporcionar informació sobre els drets de les persones en matèria de tractament de dades personals.
6. Atendre les peticions i les reclamacions formulades per les persones afectades.
7. Exercir la potestat d'inspecció.
8. Exercir la potestat sancionadora.
9. Col·laborar amb els òrgans competents en el desenvolupament normatiu i l'aplicació de normes que incideixin en el seu àmbit competencial amb l'emissió del corresponent informe preceptiu, com ara els projectes de disposicions de caràcter general de la Generalitat de Catalunya en matèria de protecció de dades de caràcter personal.
10. Respondre les consultes que li adreci qualsevol entitat del seu àmbit d'actuació i col·laborar amb aquestes entitats en la difusió de les obligacions derivades de la legislació esmentada.
11. Totes les altres funcions que li siguin atribuïdes d'acord amb les lleis.

D'altra banda, l'apdcat té l'obligació d'elaborar una memòria anual de les seves activitats que inclogui les conclusions dels seus treballs i dels expedients que hagi tramitat. Aquesta memòria s'ha de presentar davant del Parlament de Catalunya i s'ha de remetre al Govern, al Síndic de Greuges i al director o directora de l'Agència de Protecció de Dades de l'Estat.

Totes les entitats que es troben dins l'àmbit d'actuació de l'apdcat tenen l'obligació d'auxiliar, amb caràcter preferent i urgent, l'Agència Catalana de Protecció de Dades en les seves investigacions, si aquesta els ho demana.

Els òrgans de l'Agència Catalana de Protecció de Dades

Els òrgans de govern de l'Agència Catalana de Protecció de Dades són:

- la direcció
- el Consell Assessor sobre Protecció de Dades de Catalunya.

L'apdcat s'estructura de la manera següent:

a) Secretaria General

b) Assessoria Jurídica

c) Àrea del Registre de Protecció de Dades

d) Àrea d'Inspecció

La direcció

El director o la directora de l'Agència Catalana de Protecció de Dades dirigeix l'Agència i n'exerceix la representació.

Tot i que la Llei 5/2009, de 19 d'abril, estableix que el director o la directora de l'Agència serà nomenat o nomenada pel Govern, a proposta dels membres del Consell Assessor sobre Protecció de Dades de Catalunya, per un període de quatre anys, i que aquesta persona pot ser renovada, no podem oblidar que l'Estatut d'Autonomia de Catalunya ha previst que l'autoritat independent que vetlli per garantir el dret a la protecció de les dades personals en l'àmbit de les competències de la Generalitat ha de ser designada pel Parlament.

El director o la directora exerceix les seves funcions amb plena independència i objectivitat, sense subjecció a cap mandat imperatiu ni a instrucció. Anualment ha de comparèixer davant del Parlament, en la comissió pertinent, per tal d'informar sobre la seva actuació.

Tot i que no està subjecte a cap instrucció, ha d'escoltar les propostes que li faci el Consell Assessor relatives a l'exercici de les seves funcions i, si no les té en compte, ho ha de motivar.

Causes de cessament:

a) Per expiració del termini del mandat.

b) A petició pròpia.

c) Per separació acordada pel Govern, amb la instrucció prèvia del corresponent expedient, a proposta de les tres quartes parts dels membres del Consell Assessor, per incompliment de les seves obligacions, incompatibilitat, incapacitat sobrevinguda per a l'exercici de les seves funcions o condemna per delicte dolós.

El Consell Assessor de Protecció de Dades

El Consell Assessor té funcions d'assessorament, consulta, fixació de criteris i estudi.

Els membres del Consell Assessor són nomenats pel conseller o consellera de Governació a proposta de les entitats que representen. El Consell està compost pels membres següents :

a) Tres vocals designats pel Parlament, per una majoria de dos terços, a l'inici de cada legislatura.

b) Tres representants de l'Administració de la Generalitat, designats pel Govern.

c) Dos representants de l'Administració local de Catalunya, proposats per les entitats associatives d'ens locals.

d) Una persona experta en l'àmbit dels drets fonamentals, proposada pel Consell Interuniversitari de Catalunya.

e) Una persona experta en informàtica, proposada pel Consell Interuniversitari de Catalunya.

f) Un vocal en representació de l'Institut d'Estudis Catalans.

g) Un vocal en representació dels consumidors i usuaris, proposat per les organitzacions de consumidors més representatives.

h) El director o la directora de l'Institut d'Estadística de Catalunya.

Funcions del Consell Assessor:

a) Informar totes les qüestions que li sotmeti el director o la directora de l'Agència.

b) Fer propostes al director o la directora de l'Agència en relació amb l'exercici de les seves funcions.

c) Respondre les consultes que se li formulin.

d) Establir criteris en relació amb els tractaments de dades personals.

e) Realitzar estudis sobre protecció de dades personals.

f) Aprovar la plantilla del personal de l'Agència.

g) Aprovar la memòria anual de l'Agència.

El Registre de Protecció de Dades de Catalunya

El Registre de Protecció de Dades de Catalunya és un òrgan integrat a l'Agència Catalana de Protecció de Dades, segons el que estableix la Llei 5/2002, de 19 d'abril.

Les finalitats del Registre són, essencialment, garantir la publicitat dels fitxers de dades de caràcter personal existents i facilitar a la ciutadania l'exercici dels drets d'accés, rectificació, cancel·lació i oposició. Aquestes finalitats s'inscriuen dins l'objecte genèric atribuït a l'Agència Catalana de Protecció de Dades, de vetllar pel respecte dels drets fonamentals i les llibertats públiques de la ciutadania en tot allò que concerneix les operacions que formen part de l'àmbit d'actuació de l'Agència.

D'acord amb l'Estatut de l'Agència Catalana de Protecció de Dades, aprovat mitjançant el Decret 48/2003, de 20 de febrer, en els assentaments d'inscripció han de figurar les dades següents:

a) El titular i la ubicació del fitxer.

b) El responsable i/o encarregat del fitxer.

c) La finalitat i els usos del fitxer.

d) Les persones o els col·lectius afectats.

e) El procediment de recollida de dades.

f) L'estructura bàsica del fitxer i la descripció dels tipus de dades de caràcter personal que s'hi incloguin.

g) Les cessions de dades de caràcter personal.

h) Els serveis o les unitats davant els quals es puguin exercir els drets d'accés, rectificació, cancel·lació i oposició.

Les sol·licituds d'inscripció en el Registre, de rectificació de dades o de cancel·lació les han de presentar els responsables dels fitxers a l'Agència Catalana de Protecció de Dades en el termini màxim d'un mes. L'Agència ha de resoldre sobre la procedència o improcedència de la inscripció en el termini d'un mes comptat a partir de la data de la sol·licitud.

Les dades contingudes al Registre són públiques i poden ser consultades de forma gratuïta.

La competència per resoldre sobre la procedència o improcedència de les inscripcions que s'hagin de practicar en el Registre de Protecció de Dades de Catalunya la té atribuïda el/la director/a de l'Agència Catalana de Protecció de Dades, d'acord amb l'article 15.1 de l'Estatut de l'Agència.

Integració registral: el Registre de Protecció de Dades de Catalunya ha d'establir els acords de cooperació necessaris amb el Registre General de Protecció de Dades de l'Agència Espanyola de Protecció de Dades, als efectes d'integrar la informació registral i de mantenir-la actualitzada.

Dret de consulta al Registre

L'article 14 de la LOPD regula el dret de consulta al Registre general de protecció de dades i el configura com el dret de qualsevol persona a conèixer l'existència de tractaments de dades de

caràcter personal, les seves finalitats i la identitat del responsable del tractament. El Registre general és de consulta pública i gratuïta.

En termes semblants aquest dret és regulat a l'article 7.1 de la Llei 5/2002, de l'apdcat, incidint també en el caràcter gratuït de la consulta efectuada davant el Registre de Protecció de Dades de Catalunya.

En conseqüència, i a diferència del que succeeix amb els drets ARCO que atès el seu caràcter personalíssim només poden ser exercits per les persones afectades, en el dret de consulta no s'exigeix una legitimació específica, sinó que pot ser exercit per qualsevol persona, sense necessitat de justificar un dret o interès concret. La finalitat d'aquest dret de consulta és facilitar l'exercici dels drets ARCO.

Aquests registres gestionats per les autoritats de control en relació amb els quals es pot exercir el dret de consulta no recullen el contingut dels fitxers que contenen les dades personals, sinó únicament les seves característiques, com ara la identificació, el tipus de dades que contenen, els col·lectius de qui es recullen les dades, etc.

Potestat d'inspecció i sanció

La potestat d'inspecció i sanció és una de les més destacades en una autoritat independent o de control com és el cas de l'apdcat, atès que és una potestat directament vinculada a la seva finalitat i al seu objectiu principal que, tal com estableixen els articles 31 i 156 de l'EAC, és el de vetllar per tal que es respecti i garanteixi el dret a la protecció de les dades personals.

Primerament, pel que fa a la potestat d'inspecció, la Llei 5/2002, de l'apdcat, la preveu expressament a la llista de funcions de l'article 5, concretament a la lletra h). L'article 8 està dedicat a aquesta potestat i determina que l'apdcat pot inspeccionar els fitxers sotmesos al seu àmbit de competència, a fi d'obtenir totes les informacions necessàries per a l'exercici de les seves funcions. Afegeix a més que, amb aquesta finalitat, pot sol·licitar la presentació o la tramesa de documents i de dades, o bé examinar-los en el lloc on estiguin dipositats, i també inspeccionar els equips físics i lògics utilitzats, per a la qual cosa pot accedir als locals on estiguin instal·lats.

L'apartat segon de l'article 8 de la Llei 5/2002 reconeix la consideració d'autoritat pública als funcionaris de l'apdcat que exerceixen aquesta funció inspectora, de manera que gaudeixen de la presumpció de veracitat segons el que preveu l'article 137.3 de la Llei 30/1992. Així mateix, l'article 8.2 de la Llei 5/2002 obliga els funcionaris inspectors a mantenir el secret sobre les informacions de què tinguin coneixement en l'exercici de les seves funcions, fins i tot després d'haver cessat en aquestes.

Per tal d'assegurar que l'apdcat pugui desenvolupar amb normalitat aquesta potestat d'inspecció, l'article 5.3 de la Llei 5/2002 imposa a les administracions i entitats sotmeses al seu control l'obligació de prestar auxili, amb caràcter preferent i urgent, en les investigacions que es puguin dur a terme.

L'article 20 de l'Estatut de l'apdcat, aprovat pel Decret 48/2003, atribueix aquesta potestat d'inspecció a la seva Àrea d'Inspecció.

D'altra banda, la potestat sancionadora està prevista a l'article 5.i) de la Llei 5/2002 i desenvolupada als articles 16, 17 i 18 de la mateixa Llei. Així, l'article 16.2 d'aquesta Llei atribueix al director o la directora de l'apdcat, en cas de cometre's alguna de les infraccions previstes a la LOPD, la competència per dictar la resolució que estableixi les mesures que cal adoptar a fi de corregir els efectes de la infracció, sense perjudici de la possibilitat de proposar a l'òrgan competent l'inici d'actuacions disciplinàries, si escau.

Finalment, i al marge del que es veurà després en tractar el règim d'infraccions i sancions i el procediment sancionador, cal esmentar aquí la potestat d'immobilització, que apareix clarament vinculada a la potestat d'inspecció i sanció. Es tracta d'una potestat prevista a l'article 18 de la Llei 5/2002, de l'apdcat, per a casos d'una gravetat especial, en consonància amb el previst a l'article 49 de la LOPD. En concret, es refereix als supòsits constitutius d'infracció molt greu, d'utilització o

comunicació il·lícita de dades personals amb què s'atempti greument contra els drets fonamentals i les llibertats públiques o se n'impedeixi l'exercici. En aquestes situacions, s'estableix expressament que el director o la directora de l'apdcat, a més d'exercir la potestat sancionadora pot exigir als responsables el cessament de la utilització o la comunicació il·lícita de dades personals. En cas que aquest requeriment no sigui atès, es podrà, mitjançant resolució motivada, immobilitzar els fitxers de dades personals, amb l'única finalitat de restaurar els drets de les persones afectades.

Règim d'infraccions i sancions

La Llei 5/2002, de l'apdcat, no conté en el seu articulat un règim propi d'infraccions i sancions, sinó que remet al que preveu la LOPD i afegeix que la resolució del procediment corresponent la dicta el director o la directora de l'apdcat. Cal doncs anar a la LOPD, concretament als articles que van del 43 al 49. L'article 43 configura el règim de responsabilitats i determina que poden respondre de les infraccions comeses, tant els responsables del fitxer o tractament, com els encarregats del tractament. L'article 43.2 adverteix però, ja d'entrada, que en les infraccions comeses en relació amb fitxers dels quals n'és titular una Administració pública, el règim de responsabilitat serà l'específic de l'article 46.2, que després veurem.

L'article 44 conté el catàleg d'infraccions, les quals, seguint l'esquema habitual, es qualifiquen per la seva gravetat en lleus, greus i molt greus.

L'article 44.2 relaciona, en primer terme, les infraccions lleus, entre les quals destaca, pel nombre de procediments sancionadors que origina, la prevista a la lletra d) referent a l'incompliment del dret d'informació de l'article 5:

a) No atendre, per motius formals, la sol·licitud de la persona interessada de rectificació o cancel·lació de les dades personals objecte de tractament, quan legalment sigui procedent.

b) No proporcionar la informació que sol·liciti l'Agència de Protecció de Dades en l'exercici de les competències que té atribuïdes legalment, en relació amb aspectes no substantius de la protecció de dades.

c) No sol·licitar la inscripció del fitxer de dades de caràcter personal en el Registre General de Protecció de Dades, quan no sigui constitutiu d'infracció greu.

d) Recollir dades de caràcter personal dels mateixos afectats sense proporcionar-los la informació que assenyala l'article 5 d'aquesta Llei.

e) Incomplir el deure de secret que estableix l'article 10 d'aquesta Llei, llevat que constitueixi infracció greu.

L'apartat 3 de l'article 44 conté la llista de les infraccions greus, entre les quals cal subratllar la importància de la prevista en la lletra d), referent a la conculcació dels principis i les garanties de la LOPD, cosa que obliga a connectar aquesta infracció sempre amb algun principi o garantia concreta (qualitat, consentiment, seguretat, etc.):

a) Crear fitxers de titularitat pública o iniciar la recollida de dades de caràcter personal per als mateixos fitxers, sense l'autorització de disposició general, publicada en el Butlletí Oficial de l'Estat o el diari oficial corresponent.

b) Crear fitxers de titularitat privada o iniciar la recollida de dades de caràcter personal per als mateixos fitxers amb finalitats diferents de les que constitueixen l'objecte legítim de l'empresa o entitat.

c) Recollir dades de caràcter personal sense obtenir el consentiment exprés de les persones afectades, en els casos en què aquest sigui exigible.

d) Tractar les dades de caràcter personal o utilitzar-les posteriorment amb conculcació dels principis i les garanties que estableix aquesta Llei o amb incompliment dels preceptes de protecció

que imposin les disposicions reglamentàries de desplegament, quan no constitueixi infracció molt greu.

e) Impedir o obstaculitzar l'exercici dels drets d'accés i oposició i la negativa a facilitar la informació que sigui sol·licitada.

f) Mantenir dades de caràcter personal inexactes o no fer les rectificacions o les cancel·lacions de les dades que legalment siguin procedents quan siguin afectats els drets de les persones que empara aquesta Llei.

g) La vulneració del deure de guardar secret sobre les dades de caràcter personal incorporades a fitxers que continguin dades relatives a la comissió d'infraccions administratives o penals, Hisenda Pública, serveis financers, prestació de serveis de solvència patrimonial i crèdit, així com els altres fitxers que continguin un conjunt de dades de caràcter personal suficients per obtenir una avaluació de la personalitat de l'individu.

h) Mantenir els fitxers, locals, programes o equips que continguin dades de caràcter personal sense les degudes condicions de seguretat que es determinin per la via reglamentària.

i) No remetre a l'Agència de Protecció de Dades les notificacions que preveuen aquesta Llei o les seves disposicions de desplegament, i no proporcionar a l'Agència en el termini escaient tots els documents i les informacions que hagi de rebre o siguin requerits per a aquell a aquests efectes.

j) L'obstrucció de l'exercici de la funció inspectora.

k) No inscriure el fitxer de dades de caràcter personal al Registre General de Protecció Dades, quan hagi estat requerit per fer-ho pel director o la directora de l'Agència de Protecció de Dades.

l) Incomplir el deure d'informació que estableixen els articles 5, 28 i 29 d'aquesta Llei, quan les dades hagin estat recollides d'una persona diferent de la persona afectada.

Són infraccions molt greus:

a) La recollida de dades de forma enganyosa i fraudulenta.

b) La comunicació o la cessió de les dades de caràcter personal, llevat dels casos en què això estigui permès.

c) Recollir i tractar les dades de caràcter personal a què es refereix l'apartat 2 de l'article 7 quan no hi hagi el consentiment exprés de la persona afectada; recollir i tractar les dades referides a l'apartat 3 de l'article 7 quan no ho disposi una llei o la persona afectada no hi hagi consentit expressament, o violentar la prohibició que conté l'apartat 4 de l'article 7.

d) No cessar en l'ús il·legítim dels tractaments de dades de caràcter personal quan sigui requerit per fer-ho pel director o la directora de l'Agència de Protecció de Dades o per les persones titulars del dret d'accés.

e) La transferència temporal o definitiva de dades de caràcter personal que hagin estat objecte de tractament o hagin estat recollides per ser sotmeses a aquest tractament, amb destinació a països que no tinguin un nivell de protecció equiparable, sense l'autorització del director o la directora de l'Agència de Protecció de Dades.

f) Tractar les dades de caràcter personal de manera il·legítima o amb menyspreu dels principis i les garanties que els siguin aplicables, quan amb això s'impedeixi l'exercici dels drets fonamentals o s'atempti contra aquest exercici.

g) La vulneració del deure de guardar secret sobre les dades de caràcter personal a què fan referència els apartats 2 i 3 de l'article 7, així com les que hagin estat recollides per a finalitats policials sense el consentiment de les persones afectades.

h) No atendre o obstaculitzar de manera sistemàtica l'exercici dels drets d'accés, rectificació, cancel·lació o oposició.

i) No atendre de manera sistemàtica el deure legal de notificació de la inclusió de dades de caràcter personal en un fitxer.

L'article 45 de la LOPD regula les sancions seguint el mateix esquema de classificació d'acord amb la gravetat i determina els imports de les multes, que són molt elevats. Concretament, aquests imports -previstos a la LOPD en pessetes i adaptats aquí a l'euro- són els següents:

Lleus: de 601,01 € a 60.121,21 €

Greus: de 60.121,21 € a 300.506,05 €

Molt greus: de 300.506,05 € a 601.012,10 €.

L'article 45.4 de la LOPD disposa que la sanció que s'imposi s'ha de graduar d'acord amb un seguit de circumstàncies que l'article preveu, per tal de respectar el principi de proporcionalitat. En aquest precepte es reiteren algunes de les circumstàncies establertes amb caràcter general a l'article 131 de la Llei 30/1992, que fa referència precisament al principi de proporcionalitat en la potestat sancionadora, i s'hi afegeixen algunes d'específiques que tenen incidència en l'àmbit de la protecció de dades, com ara el volum dels tractaments de dades efectuats o els beneficis obtinguts.

L'article 45.5 de la LOPD preveu la possibilitat de rebaixar en un grau la sanció que s'ha imposar quan, per les circumstàncies concurrents, s'aprecia una disminució qualificada de l'imputat o de l'antijuricitat del fet. La jurisprudència s'ha vist obligada a precisar que aquest instrument té un caràcter excepcional, només per als casos en què concorrin les circumstàncies previstes al precepte, sense que es pugui aplicar de forma generalitzada, tot i que és comprensible que les entitats sancionades l'invoquin sovint, atès el caràcter tan elevat de les multes previstes a la LOPD.

L'article 46 de la LOPD ha previst un règim sancionador específic per al cas de les infraccions comeses en fitxers dels quals siguin responsables les administracions públiques. En aquest cas, no s'imposa una sanció econòmica, sinó que en la resolució que declara una eventual infracció, s'hi han d'establir les mesures que escau adoptar perquè cessin o es corregeixin els efectes de la infracció. En aquesta resolució que declara la infracció es pot proposar a l'òrgan responsable l'inici d'actuacions disciplinàries, si són procedents. Així mateix, el precepte disposa que la resolució per la qual es declara la comissió d'una infracció en fitxers de les administracions públiques s'ha de comunicar al Defensor del Pueblo, que en el cas de l'apdcat s'ha d'entendre que és al Síndic de Greuges, tal com preveu expressament l'article 16.4 de la Llei 5/2002, de l'apdcat.

Per acabar amb el règim d'infraccions i sancions, l'article 47 de la LOPD regula la institució de la prescripció, i ho fa en els termes següents:

- Pel que fa a les infraccions, prescriuen al cap de tres anys, dos anys i un any, segons si són molt greus, greus o lleus, respectivament. Aquest termini comença a comptar el dia en què s'havia comès la infracció, s'interromp amb la notificació de l'inici del procediment, i es reprèn si està paralitzat durant més de sis mesos per causes no imputables al presumpte infractor.
- Pel que fa a les sancions, prescriuen en els mateixos terminis que les infraccions. Aquest termini comença a comptar des de l'endemà del dia en què adquireix fermesa la resolució per la qual s'imposa la sanció, s'interromp amb la notificació a la persona sancionada de l'inici del procediment d'execució, i es reprèn si aquest procediment està paralitzat durant més de sis mesos per causa no imputable a la persona sancionada.

Unitat 6: L'estatut de l'encarregat del tractament

Concepte

Amb la LOPD apareix per primera vegada definida a la norma una situació que es produeix de forma molt habitual en la pràctica: la del tercer que presta serveis per compte d'un altre i que, per fer-ho, ha de tenir accés a dades personals. Des de la perspectiva de la protecció de dades es parla de l'encarregat del tractament i apareix definit a l'article 3.g de la LOPD com:

"la persona física o jurídica, l'autoritat pública, el servei o qualsevol altre organisme que, sol o conjuntament amb altres, tracti dades personals per compte del responsable del tractament".

Aquesta definició s'amplia en el RLOPD, concretament a l'article 5.i, en què s'estableix com a encarregat del tractament:

"la persona física o jurídica, pública o privada, o l'òrgan administratiu que, sol o conjuntament amb altres, tracti dades personals per compte del responsable del tractament o del responsable del fitxer, com a conseqüència de l'existència d'una relació jurídica que l'hi vincula i delimita l'àmbit de la seva actuació per a la prestació d'un servei. També poden ser encarregats del tractament els ens sense personalitat jurídica que actuïn en el tràfic com a subjectes diferenciats".

Hem de tenir present que les persones vinculades laboralment al responsable del fitxer no seran considerades encarregades del tractament.

Exemples de possibles encarregats del tractament:

- Una gestoria que fa les nòmines d'un ajuntament.
- Una diputació que gestiona el padró per compte d'un ajuntament.
- Una empresa pública que té delegada la prestació d'un determinat servei públic.
- Un departament que té encomanada la prestació d'un determinat servei per compte d'un altre.

En tot cas, cal tenir present que no necessàriament totes les situacions descrites han de configurar l'existència d'un encarregat del tractament, sinó que això vindrà determinat per la configuració que es doni a la relació jurídica que s'estableixi entre ambdues entitats.

Regulació de les relacions entre el responsable del fitxer i l'encarregat del tractament

La configuració d'un tercer com a encarregat del tractament té una sèrie de conseqüències pràctiques molt importants. Així, per exemple, no es considera cessió de dades el traspàs d'informació cap a aquell que s'ha configurat com l'encarregat del tractament, és a dir, no li és d'aplicació el règim jurídic regulat als articles 11 i 21 de la LOPD.

Però, per tal que es pugui aplicar la regulació establerta per a l'encarregat del tractament, cal que es compleixin els requisits de l'article 12 de la LOPD i del 20 del RLOPD:

- L'accés a les dades personals ha de ser necessari per a la prestació d'un servei al responsable del tractament.
- El servei prestat per l'encarregat del tractament pot tenir o no caràcter remunerat i ser temporal o indefinit.
- La realització de tractaments per compte de tercers s'ha de regular en un contracte que ha de constar per escrit o alguna altra forma que permeti acreditar-ne la concertació i el contingut. En aquest contracte s'ha de fer constar de manera expressa:
  - Que l'encarregat del tractament només tractarà les dades d'acord amb les instruccions del responsable del tractament.
  - Que no les pot aplicar ni utilitzar amb una finalitat diferent de la que figuri en el contracte.
  - Que no pot comunicar-les a altres persones, ni tan sols per conservar-les. Aquest últim requisit es matisarà amb la possibilitat de subcontractació que es veurà en el proper punt.
  - Les mesures de seguretat que cal implantar i que són exigibles atenent al tipus de dades personals que s'han de tractar. Als articles 82 i 83 del RLOPD s'estableixen algunes especificacions respecte de l'encarregat del tractament que es veuran en l'apartat de les mesures de seguretat.
  - Si, una vegada complerta la prestació contractual, les dades de caràcter personal han de ser destruïdes o tornades al responsable del tractament, i també qualsevol suport o document en què consti alguna dada de caràcter personal objecte del tractament. Això, sens perjudici del que veurem més endavant en relació amb la possibilitat de conservació de les dades per part de l'encarregat del tractament.
  - El mecanisme mitjançant el qual el responsable del tractament vetllarà perquè l'encarregat del tractament compleixi les garanties per al compliment del que disposa la normativa de protecció de dades

Cal recordar que es considera que hi ha comunicació de dades quan l'accés tingui per objecte l'establiment d'un nou vincle entre qui accedeix a les dades i la persona afectada.

D'altra banda, en el contracte també es pot preveure que la persona afectada exerceixi els seus drets d'accés, rectificació, cancel·lació i oposició davant de l'encarregat del tractament. En aquest cas, caldrà que es defineixi si:

- l'encarregat ha de donar trasllat de la sol·licitud al responsable, a fi que aquest la resolgui, o si
- l'encarregat ha d'atendre, per compte del responsable, les sol·licituds d'exercici dels seus drets per part de les persones afectades.

Subcontractació de serveis

Tot i el que hem vist en el punt anterior respecte a la no-possibilitat, per part de l'encarregat del tractament, de comunicar a tercers les dades objecte del servei que li ha estat contractat, ni tant sols per a la seva conservació (excepte si es té l'autorització del responsable del tractament i es contracta en nom i per compte d'aquest), a l'article 21 del RLOPD es regula la possibilitat de subcontractar els serveis si es compleixen una sèrie de requisits. Podem distingir dos supòsits:

- Que s'especifiquin en el contracte els serveis que puguin ser objecte de subcontractació i, si és possible, l'empresa amb la qual s'ha de subcontractar.
- Que no s'identifiqui en el contracte l'empresa amb la qual s'ha de subcontractar. Aleshores, és necessari que l'encarregat del tractament comuniqui al responsable les dades que la identifiquin abans de procedir a la subcontractació.

En qualsevol dels dos casos, és necessari que:

- El tractament de dades de caràcter personal per part del subcontractista s'ajusti a les instruccions del responsable del fitxer.
- L'encarregat del tractament i l'empresa subcontractista formalitzin el contracte en els termes previstos a l'article anterior.

En tot cas, si durant la prestació del servei és necessari subcontractar-ne una part i aquesta circumstància no s'ha previst en el contracte, s'han de sotmetre al responsable del tractament els aspectes assenyalats a l'apartat anterior.

Finalment, cal indicar que aquelles entitats subjectes a la Llei 30/2007, de 30 d'octubre, de contractes del sector públic, han de tenir en compte el que aquesta norma estableix a la disposició addicional 31 respecte dels contractes que impliquen tractaments de dades personals. En l'apartat tercer d'aquesta disposició s'indica que si un tercer tracta dades personals per compte del contractista, s'han de complir els requisits següents:

1. El tractament de dades personals s'ha d'especificar en el contracte signat per l'entitat contractant i el contractista.
2. El tractament de dades personals s'ha d'ajustar a les intruccions del responsable del tractament.
3. El contractista i el tercer han de formalitzar un contracte en els termes que preveu l'article 12 de la LOPD.

D'aquesta manera, el tercer també tindrà la consideració d'encarregat del tractament.

Conservació de les dades per part de l'encarregat del tractament

Tot i que a l'article 12 de la LOPD s'estableix que, una vegada complerta la prestació contractual, les dades de caràcter personal han de ser destruïdes o tornades al responsable del tractament, i també qualsevol suport o document en què consti alguna dada de caràcter personal objecte del tractament, a l'article 22 del RLOPD s'ha flexibilitzat aquesta obligació en dos casos:

- Quan hi hagi una previsió legal que n'exigeixi la conservació. En aquest cas s'ha de procedir a la devolució de les dades amb la garantia del responsable del fitxer de la conservació esmentada.
- Quan l'encarregat del tractament hagi de conservar les dades, degudament bloquejades, perquè es puguin derivar responsabilitats de la seva relació amb el responsable del tractament.

Responsabilitat de l’encarregat del tractament

En cas que l’encarregat del tractament destini les dades a finalitats diferents a les establertes en el contracte, les comuniqui o les utilitzi incomplint les estipulacions d'aquest contracte, serà considerat responsable del tractament i haurà de respondre de les infraccions en què hagi incorregut personalment.

No obstant això, l’encarregat del tractament no incorre en responsabilitat quan, amb la indicació prèvia i expressa del responsable, comunica les dades a un tercer designat per aquell, a qui ha encomanat la prestació d’un servei conforme al que s'exposa en aquesta unitat.

Quan es compleixin els requisits establerts a l’article 21.2 del RLOPD per a la subcontractació de serveis, el subcontractista és considerat encarregat del tractament i li és aplicable el que s'indica anteriorment.

Unitat 7: La implantació de mesures de seguretat

Introducció

L'article 17 de la Directiva 95/46/CE [1] del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades, preveu que **qui tracta dades personals té l'obligació de protegir la informació de caràcter personal**, una obligació que la Directiva considera una condició de legalitat dels tractaments de dades de caràcter personal, ja que aquest article 17 se situa al capítol II de la Directiva, el que tracta sobre les *"Condicions generals per a la licitud del tractament de dades personals"*.

> Article 17. Seguretat del tractament.
>
> 1. Els Estats membres estableixen l'obligació del responsable del tractament d'aplicar les mesures tècniques i d'organització adequades per a la protecció de les dades personals contra la destrucció, accidental o il·lícita, la pèrdua accidental i contra l'alteració, la difusió o l'accés no autoritzats, en particular quan el tractament inclogui la transmissió de dades dins d'una xarxa, i contra qualsevol altre tractament il·lícit de dades personals.

El «principi de seguretat», en el context de la protecció de dades de caràcter personal, implica la imposició al responsable del tractament d'un «deure de protecció» de les dades personals que tracta.

La Directiva considera que, per a una adequada salvaguarda dels drets i les llibertats, cal obligar els responsables de tractaments a adoptar mesures tècniques i d'organització que protegeixin la informació de caràcter personal, ponderant aspectes com l'estat de la tecnologia en cada moment o la naturalesa de les dades a protegir (considerant 46).

1 Directiva 95/46/CE - enllaç extern

L'article 9 de la Llei orgànica 15/1999[2], de 13 de desembre, de protecció de dades de caràcter personal (LOPD), recull aquest principi de seguretat.

> Article 9. Seguretat de les dades.
>
> 1. El responsable del fitxer i, si s'escau, l'encarregat del tractament han d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposats, tant si provenen de l'acció humana o del medi físic o natural.
>
> 2. No s'han de registrar dades de caràcter personal en fitxers que no compleixin les condicions que es determinin per via reglamentària en relació amb la seva integritat i seguretat i a les dels centres de tractament, locals, equips, sistemes i programes.
>
> 3. S'han d'establir per reglament els requisits i les condicions que han de complir els fitxers i les persones que intervinguin en el tractament de les dades a què es refereix l'article 7 d'aquesta Llei.

El principi de seguretat es concreta en el deure del responsable del tractament i, si s'escau, de l'encarregat del tractament de dur a terme les accions necessàries per protegir les dades de caràcter personal dels riscos derivats del seu tractament i de la naturalesa de les dades tractades.

El reglament a què es refereix l'article 9.3 és el que aprova el Reial decret 1720/2007[3], de 21 de desembre (RLOPD), que desenvolupa el principi de seguretat que recullen els articles 9 de la LOPD i 17 de la Directiva 95/46/CE, establint els requisits i condicions de seguretat de fitxers i tractaments de dades personals.

El Reial decret 1720/2007 dedica el títol VIII a *"les mesures de seguretat en el tractament de dades de caràcter personal"*. En l'exposició de motius del reglament la seguretat és considera *"un aspecte essencial per a la tutela del dret fonamental a la protecció de dades"*.

Les mesures de seguretat es descriuen en el reglament de desenvolupament de la LOPD al llarg de 36 articles (articles del 79 al 114) que, juntament amb altres referències a les mesures de seguretat, representen aproximadament un 30% del conjunt del reglament.

Per últim, cal tenir en compte que la LOPD preveu una infracció directament relacionada amb la falta de mesures de seguretat o amb la seva ineficàcia:

Infraccions greus (art. 44.3):
"h) Mantenir els fitxers, locals, programes o equips que continguin dades de caràcter personal sense les degudes condicions de seguretat que es determinin per la via reglamentària."

2 LOPD - enllaç extern
3 RLOPD - enllaç extern

Seguretat de la informació

Abans d'aprofundir en les qüestions relatives a les mesures de seguretat, tècniques i organitzatives, que cal adoptar en relació amb la protecció de dades de caràcter personal, convé fer una aproximació a un concepte més ampli com és el de la seguretat de la informació.

En aquest context, la seguretat té com a principal funció generar confiança, és a dir, els usuaris dels sistemes d'informació han de confiar que:

1.la informació estarà disponible quan es necessiti (**disponibilitat**)

2.la informació no serà modificada sense control (**integritat**)

3.la informació es mantindrà accessible només per a aquells que l'han de conèixer (**confidencialitat**).

En determinades circumstàncies també serà necessari garantir la identitat de qui interactua amb els sistemes d'informació (autenticitat) i disposar d'informació que permeti conèixer què ha passat en un sistema d'informació (auditabilitat o traçabilitat).

Seguretat i sistemes d'informació

De forma genèrica s'han de protegir les persones, béns i serveis que formen part d'una organització, sigui pública o privada. En conseqüència, les mesures de seguretat s'han d'aplicar a les dades, els processos, les aplicacions, els sistemes operatius, el maquinari, les comunicacions, els suports d'informació, les instal·lacions físiques, els locals i el personal; en definitiva, a tots els elements que fan funcionar o estan involucrats en els sistemes d'informació.

El RLOPD defineix què és un sistema d'informació (article 5.2.m): "conjunt de fitxers, tractaments, programes, suports i, si s'escau, equipaments utilitzats per al tractament de dades personals".

Una altra qüestió relacionada amb els sistemes d'informació té a veure amb el sistema de tractament, és a dir: les mesures de seguretat no s'apliquen exclusivament al tractament automatitzat de la informació, sinó també als tractaments no automatitzats.

En aquest sentit, també pot ser d'utilitat la definició de sistema de tractament de l'article 5.2.n del RLOPD: "manera en què s'organitza o utilitza un sistema d'informació. Segons el sistema de tractament els sistemes d'informació podran ser automatitzats, no automatitzats o parcialment automatitzats".

Les mesures de seguretat, siguin tècniques o organitzatives, han de protegir la informació personal en tot moment i en qualsevol ubicació .

Anàlisi de riscos

L'anàlisi de riscos, en el context de la seguretat de la informació, és un procés sistemàtic per fer una estimació del nivell de risc al qual estan exposades les diferents parts (actius) que fan funcionar o estan involucrades en els sistemes d'informació.

Aquest procés sistemàtic intenta identificar els perills (amenaces), és a dir, concretar quins incidents (voluntaris o accidentals) poden afectar les dades, el funcionament dels sistemes d'informació o el seu valor.

També s'avalua la probabilitat que les amenaces es materialitzin i fins a quin punt afectarien els sistemes i les dades (impacte).

Les mesures de seguretat implantades son salvaguardes que poden reduir la probabilitat que succeeixi l'incident o poden disminuir els efectes negatius en cas que es produís l'incident.

Quan es parla de gestionar el risc, el que es vol fer és reduir el nivell de risc que es té i això s'aconsegueix implantant noves salvaguardes o millorant les existents.

Per a les administracions públiques existeix una metodologia d'anàlisi de riscos anomenada MAGERIT (Metodologia d'Anàlisi i Gestió de Riscos dels Sistemes d'Informació) creada pel Consejo Superior de Administración Electrónica[4].

Difícilment podrem prendre decisions sobre seguretat de la informació sense saber què hem de protegir, de quins perills ens hem de protegir, ni quines poden ser les conseqüències en cas que es produeixi un incident de seguretat.

Planificació de la seguretat

La seguretat s'ha de planificar: s'han d'establir uns objectius de seguretat i verificar que s'assoleixen. Una vegada realitzada l'anàlisi de riscos, estem en disposició de conèixer quines accions de seguretat hem de dur a terme (projectes de seguretat).

Podrem prioritzar els projectes de seguretat a fi d'anar reduint el nostre risc segons un pla prèviament definit.

Implantació i gestió de la seguretat

La seguretat requereix ser documentada per garantir la seva correcta implantació i ha de ser gestionada per garantir la seva eficàcia. L'article 88 del RLOPD preveu que les mesures de seguretat relacionades amb la protecció de dades de caràcter personal siguin concretades en el que es coneix com a **document de seguretat**.

L'article 88.1 obliga el responsable del fitxer o del tractament a elaborar un document de seguretat que reculli les mesures tècniques i organitzatives que siguin d'aplicació, segons la normativa vigent, als tractaments i fitxers de la seva responsabilitat, i que seran d'obligat compliment per al personal amb accés als sistemes d'informació.

La seguretat s'ha de gestionar. Tal com exigeix l'article 88.7, el document de seguretat s'ha de mantenir en tot moment actualitzat, amb la finalitat de fer efectiva aquesta gestió. El RLOPD preveu la figura del **responsable de seguretat**, que s'encarrega de coordinar i controlar les mesures de seguretat definides en el document de seguretat (article 95).

El document de seguretat i el responsable de seguretat son claus per a una implantació i gestió correcta de les mesures de seguretat.

Seguretat i prevenció

La prevenció està especialment indicada per a l'àmbit de la protecció de dades de caràcter personal, ja que quan es lesiona aquest dret fonamental, els efectes de la vulneració són habitualment de caràcter irreversible.

4 MAGERIT - enllaç extern

Una vegada la intimitat o privadesa han estat violentades, la reparació del dret de la persona afectada resulta impossible o poc efectiva.

Fins i tot per al responsable del tractament, encara que no arribi a produir-se la declaració d'infracció, el fet de veure's involucrat en un incident de seguretat amb dades personals pot tenir conseqüències sobre la seva imatge o la seva credibilitat que provoquin una pèrduda de confiança difícil de recuperar.

Per això, tot allò que permeti evitar que es produeixi l'incident serà molt més eficient, tant per als afectats com per als responsables dels fitxers o tractaments.

La prevenció, adoptant mesures tècniques i organitzatives apropiades tant en el moment de la concepció del sistema d'informació com durant tot el cicle de vida de la informació tractada, és el que realment pot garantir un adequat clima de confiança i seguretat.

Els instruments preventius poden ser de tipus procedimental, organitzatiu o tecnològic i s'orienten a avançar-se als possibles incidents.

Marcs de referència

El conjunt de la normativa que regula el dret a la protecció de dades personals és d'obligat compliment per als responsables dels fitxers i tractaments inclosos en l'àmbit d'aplicació de la legislació.

Ara bé, existeixen altres marcs de referència, de caràcter voluntari, que també es poden tenir en compte i que, en forma d'estàndards internacionals, proporcionen nivells de protecció de la informació que poden arribar a ser conformes als requeriments de seguretat definits per la legislació en matèria de protecció de dades de caràcter personal.

Podem considerar com a punt de partida l'estàndard britànic BS 7799, de l'any 1995, que recollia un conjunt de bones pràctiques per a la gestió de la seguretat de la informació.

L'any 2000, la primera part d'aquest estàndard (BS 7799-1) va ser adoptada per la ISO[5], sota la denominació d'ISO 17799 (ara ISO 27002); el 2005, la segona part de l'estàndard (BS 7799-2) es va publicar com a norma ISO 27001.

ISO/IEC 27000[6] és un conjunt d'estàndards publicats, o en fase de desenvolupament, per la ISO (International Organization for Standardization) i la IEC (International Electro-technical Commission), que proporciona un marc de gestió de la seguretat de la informació que pot ser utilitzat per qualsevol tipus d'organització, sigui pública o privada.

Seguretat i protecció de dades personals

A l'inici d'aquest mòdul ja s'ha posat de relleu la importància de les mesures de seguretat per a la protecció de les dades de caràcter personal.

La legislació vigent parteix de la base que, per a una adequada salvaguarda dels drets i les llibertats, cal obligar els responsables de tractaments a adoptar mesures tècniques i d'organització que protegeixin la informació de caràcter personal, ponderant aspectes com l'estat de la tecnologia en cada moment o la naturalesa de les dades a protegir.

5 ISO - enllaç extern
6 ISO 27000 - enllaç extern

Principi de seguretat

També hem identificat la importància del principi de seguretat, que es concreta en el deure del responsable del tractament i, si s'escau, de l'encarregat del tractament, de dur a terme les accions necessàries per protegir les dades de caràcter personal.

Les mesures de seguretat, en relació amb les dades personals, han d'evitar (article 9.1 LOPD):

- L'alteració no prevista de la informació (sigui accidental o voluntària)
- La pèrdua de la informació de caràcter personal
- El tractament no autoritzat de les dades
- L'accés a les dades per part de persones no autoritzades

El RLOPD regula les mesures de seguretat, en el títol VIII, de la manera següent:

- Primer preveu unes mesures de caràcter general que afecten tot tipus de tractaments i tots els nivells de seguretat (capítols I i II, articles del 79 al 88).
- Continua la regulació específica de les mesures de seguretat per als tractaments automatitzats, i s'utilitza l'assignació de nivells de seguretat d'acord amb el tipus de dades tractades: nivell bàsic, nivell mitjà i nivell alt (capítol III, articles del 89 al 104).
- Finalment es regulen les mesures de seguretat per als tractaments no automatitzats, i se segueix el mateix esquema dels 3 nivells de seguretat (capítol IV, articles del 105 al 114).

L'objecte de protecció

Les mesures de seguretat s'han d'aplicar als (article 9.2 de la LOPD):

- centres de tractament
- locals
- equips
- sistemes
- programes

En definitiva, cal aplicar-les a tots aquells elements físics i lògics que intervenen en el tractament de les dades de caràcter personal.

Amb caràcter general, les mesures de seguretat han de protegir les dades de caràcter personal amb independència de la seva ubicació o del sistema de tractament: allà on hi hagi informació personal ha d'estar implantada la corresponent mesura de seguretat.

Classificació de la informació i aplicació dels nivells de seguretat

Com sabem les mesures de seguretat que cal aplicar en cada cas?

Les mesures de seguretat s'organitzen en nivells: concretament, hi ha 3 nivells de seguretat (bàsic, mitjà i alt) que s'apliquen d'acord amb el tipus de dades objecte de tractament (articles 80 i 81 del RLOPD). Hem d'analitzar quines dades conté el fitxer o gestiona el tractament per determinar les mesures que cal aplicar.

Per a cada nivell es descriuen una sèrie de requeriments de protecció de les dades, és a dir, quina protecció ha de proporcionar la mesura de seguretat; els nivells son acumulatius, de manera que, per exemple, a unes dades de nivell mitjà se'ls apliquen també les mesures de seguretat de nivell bàsic.

L'article 81 determina quin nivell de protecció s'ha d'aplicar a cada tipus d'informació:

1. A tots els tractaments de dades de caràcter personal cal aplicar-los les mesures de seguretat de **nivell bàsic**.
2. Les mesures de seguretat de **nivell mitjà** s'han d'aplicar als tractaments:
   - relatius a la comissió d'infraccions administratives o penals;
   - relacionats amb la prestació de serveis d'informació sobre solvència patrimonial i crèdit;
   - que siguin responsabilitat de les administracions tributàries, en relació amb l'exercici de potestats tributàries;
   - que siguin responsabilitat de les entitats financeres, en relació amb la prestació de serveis financers;
   - que siguin responsabilitat de les entitats gestores i serveis comuns de la Seguretat Social, relacionats amb l'exercici de les seves competències;
   - que siguin responsabilitat de les mútues d'accidents de treball i malalties professionals de la Seguretat Social, o
   - que continguin un conjunt de dades de caràcter personal que proporcionin una definició de les característiques o de la personalitat de les persones i que permetin avaluar determinats aspectes de la seva personalitat o del seu comportament.
1. Les mesures de seguretat de **nivell alt** s'han d'aplicar als tractaments que tractin dades sobre:
   - ideologia,
   - afiliació sindical,
   - religió,
   - creences,
   - origen racial,
   - salut,
   - vida sexual,
   - aquells que continguin o es refereixin a dades obtingudes per a finalitats policials, sense consentiment de les persones afectades, o
   - aquells que tractin dades derivades d'actes de violència de gènere.

Hi ha algunes especialitats i excepcions en l'aplicació d'aquest esquema general de determinació del nivell de seguretat:

- Les **dades de trànsit i localització** que tractin els operadors que prestin serveis de telecomunicacions electròniques disponibles per al públic o explotin xarxes públiques de comunicacions electròniques són inicialment considerades dades de nivell mitjà, però també han d'estar protegides amb una mesura concreta de nivell alt, la prevista a l'article 103 del RLOPD (el registre d'accessos).
- Quan es tractin dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual, amb l'única finalitat de fer **transferències de diners** a entitats de les quals són associades o membres les persones de les quals es tracten aquests tipus de dades, o si es tracta d'un **fitxer o tractament** en què **apareixen de forma incidental o accessòria** aquest tipus de dades sense que tinguin relació amb la finalitat del fitxer o tractament. Aleshores, només s'han d'aplicar les mesures de seguretat previstes al nivell bàsic.

- Si es tracta d'un fitxer o un tractament que utilitza dades de salut que es refereixen exclusivament a un **grau de discapacitat** o només a la **declaració de la discapacitat o invalidesa** de la persona afectada, i sempre que sigui necessari tractar aquesta dada per donar **compliment a uns deures públics**. En aquest cas, seran suficients les mesures de seguretat de nivell bàsic per a aquest fitxer o tractament.

Els 3 nivells de seguretat previstos (bàsic, mitjà i alt) s'apliquen d'acord amb el tipus de dades contingudes en el fitxer o amb el tipus de dades que són objecte de tractament. Les mesures de seguretat de cada nivell són mínims exigibles i tenen caràcter acumulatiu.

Tipus de tractaments: automatitzats i no automatitzats

Les mesures de seguretat tenen per objecte protegir la informació personal, amb independència del sistema utilitzat per al tractament.

El fet que fins l'any 2008 no entrés en vigor el Reglament de desenvolupament de la LOPD i que fins llavors les mesures de seguretat estiguessin regulades en el Reglament de mesures de seguretat dels fitxers automatitzats aprovat pel Reial decret 994/1999, va provocar que en certa mesura es considerés, erròniament, que l'obligació d'implantació de mesures de seguretat afectava exclusivament els tractaments automatitzats.

En aplicació de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, el principi de seguretat és aplicable a qualsevol sistema de tractament de les dades personals, automatitzat i no automatitzat, si bé és cert que no existia una regulació específica de les mesures de seguretat per als tractaments no automatitzats que ara sí que existeix amb el Reglament que aprova el Reial decret 1720/2007.

És útil tenir en compte la definició que fa el mateix Reglament a l'article 5.1.n de **fitxer no automatitzat**: "conjunt de dades de caràcter personal organitzat de forma no automatitzada i estructurat conforme a criteris específics relatius a persones físiques, que permetin accedir sense esforços desproporcionats a les dades personals d'una persona concreta".

Documentant la seguretat

Totes les mesures de seguretat que el responsable del fitxer o tractament està obligat a implantar han d'estar documentades. L'article 88 del RLOPD regula el **document de seguretat**.

El responsable del fitxer o del tractament ha d'elaborar un document que reculli totes les mesures de seguretat, tant tècniques com organitzatives, a les quals estigui obligat per la legislació per tal de protegir les dades que són de la seva responsabilitat.

El Reglament deixa en mans del responsable del fitxer o tractament decidir la forma d'aquest document, és a dir, pot optar per fer un únic document per a tots els tractaments, fer-ne un per a cada fitxer o tractament, tenir un cos documental central i després anar afegint annexos, etc.

El que sí que regula el Reglament són els **continguts mínims** del document de seguretat.

Sempre que es tractin dades personals, amb independència del nivell de protecció requerit, el document de seguretat haurà d'incloure els continguts següents:

- Una descripció de l'àmbit d'aplicació de les mesures de seguretat contingudes en el document de seguretat, a més d'especificar què és el que s'està protegint.
- Un recull de totes les mesures, les normes, els procediments, les regles, els estàndards, etc. que ha previst el responsable del fitxer o tractament per garantir el nivell de seguretat aplicable a les dades.

- Una descripció de totes les funcions i obligacions del personal en relació amb el tractament de dades personals (no hem d'oblidar que és un document de caràcter intern que ha de ser conegut pels membres de l'organització en totes aquelles parts que els afecten en qualitat de personal amb accés a dades personals).
- L'estructura dels fitxers amb dades personals i la descripció dels sistemes d'informació que tracten les dades.
- Els procediments de notificació, gestió i resposta als incidents que puguin afectar a dades personals.
- Els procediments per realitzar les còpies de seguretat i la recuperació de les dades.
- Totes aquelles mesures relacionades amb el transport de suports d'informació i documents, la seva destrucció i, si s'escau, la seva reutilització.

Addicionalment, en cas de fitxers o tractaments al quals sigui d'aplicació el nivell mitjà de mesures de seguretat, el document de seguretat haurà de contenir:

- La identificació del responsable o els responsables de seguretat.
- Els controls periòdics que es realitzaran per verificar el compliment del que preveu el document, és a dir, les auditories que s'han de realitzar cada 2 anys.

Els articles 88.5 i 88.6 regulen les particularitats de la gestió del document de seguretat quan existeix un encarregat de tractament.

Tots els fitxers o tractaments de dades personals, amb independència del nivell de seguretat requerit pel tipus de dades, han de tenir el seu document de seguretat, el qual ha de ser conegut pel personal amb accés a dades personals en aquelles parts que l'afecti. El document de seguretat ha d'estar en tot moment actualitzat.

Mesures de seguretat

Aquesta unitat la dedicarem a revisar totes les mesures de seguretat que recull el títol VIII del Reglament de desplegament de la LOPD.

La metodologia que s'ha seguit per descriure les mesures de seguretat està centrada en allò que han de protegir, i en cada cas s'indica el nivell de mesura de seguretat i una breu descripció de la mesura de seguretat.

Conceptes clau: definicions

L'article 5.2 del RLOPD recull la definició de conceptes relacionats directament amb la comprensió i interpretació del títol VIII del Reglament.

- **Accessos autoritzats**: són els permisos d'ús o accés que tenen concedits cadascun dels usuaris que tracten dades personals.

- **Autenticació**: és el mecanisme tècnic que s'utilitza per comprovar que un usuari, quan interactua amb un sistema d'informació, és qui diu que és. En aquest procés és on s'utilitzen els noms d'usuari i les paraules de pas o codis d'accés (contrasenyes dinàmiques o estàtiques), certificats digitals o fins i tot sistemes biomètrics.
- **Paraula de pas** (contrasenya): acompanya la identitat d'un usuari (codi d'usuari) a fi de verificar que qui vol utilitzar un nom d'usuari, si també coneix el codi d'aquell usuari (que només ha de conèixer ell), és la persona autoritzada a usar el codi d'usuari i els recursos per als quals té autoritzat l'accés. D'aquesta manera queda garantit el procés d'autenticació.
  La seva "robustesa", és a dir, el grau de dificultat que la paraula de pas sigui "endevinada" per tercers, pot dependre de: la seva longitud (nombre de caràcters), la seva composició (combinació de nombres, lletres i signes), la seva aleatorietat (codi triat per l'usuari, seleccionat de forma aleatòria entre uns codis prèviament assignats a l'usuari o bé codis generats en cada procés d'autenticació).
- **Control d'accés**: són els mecanismes que permeten accedir al sistema d'informació i a les funcionalitats o permisos que té l'usuari, una vegada el seu accés ha estat verificat, és a dir, autenticat.
- **Còpia de seguretat**: és el resultat d'executar un procés que reprodueix (fa una còpia) la informació en un dispositiu extern a aquell en què habitualment es tracta la informació. El resultat de la còpia és un conjunt d'informació en un suport extern, que pot estar protegit mitjançant un codi xifrat o simplement comprimit per ocupar menys espai. En tot cas, la qüestió clau és que la informació pugui ser recuperada, és a dir, que si sorgeix la necessitat puguin tornar a ser incorporades al sistema d'informació les dades que van ser reproduïdes o copiades.
- **Document**: la definició del Reglament és suficientment clara i àmplia. En ocasions els sistemes de informació estaran basats en documents, la condició principal és que siguin conjunts d'informació que puguin tractar-se un per un. En cas de tractaments automatitzats de documents, es pot considerar sinònim de fitxer.
- **Fitxers temporals**: aquesta definició fa referència a una realitat dels actuals sistemes d'informació, els quals permeten molta flexibilitat als usuaris (o processos) quant a possibilitats d'extreure informació, encara que sigui de forma puntual i temporal, a fi de realitzar tractaments específics que en realitat són instrumentals o accessoris del tractament principal. Òbviament a aquests conjunts d'informació i tractaments temporals els són d'aplicació tots els principis de protecció de dades, també les mesures de seguretat.
- **Identificació**: és el procediment que se segueix per assignar a un usuari o a un procés les seves credencials a l'efecte de la seva posterior autenticació en el sistema.
- **Incidència**: hem d'entendre que qualsevol circumstància o fet que pugui afectar la disponibilitat, autenticitat, integritat, confidencialitat o auditabilitat de les dades de caràcter personal ha de tractar-se com a incidència. En termes de l'article 9 de la LOPD, incidència és qualsevol fet que pugui alterar la informació, provocar la seva pèrdua o permetre accessos o tractaments no autoritzats.
- **Perfil d'usuari**: es tracta d'un aspecte purament organitzatiu sobre la manera en què els permisos d'accés es gestionen. Habitualment les eines de control d'accés incorporen la funció de definir grups d'usuaris quan dintre d'una organització diferents usuaris poden portar a terme les mateixes funcions amb les mateixes dades. Els usuaris s'agrupen, però cadascun disposa del seu usuari.
- **Recurs**: aquesta definició necessita poca explicació, en tot cas tenir clar que inclou dades (informació), aplicacions (processos), tecnologia, locals, persones i procediments, etc.
- **Responsable de seguretat**: aquesta definició tampoc dóna marge a interpretació. Cal destacar que existeix una assignació formal de la funció de seguretat i que aquesta funció pot estar desenvolupada per més d'una persona, per a un o per a diversos tractaments, i que aquestes

persones depenen d'un responsable del tractament que és qui determina quines han de ser les mesures de seguretat que han de ser coordinades i controlades pel responsable de seguretat.

- **Sistema d'informació**: aquesta definició inclou la relació dels recursos que formen part d'un sistema d'informació, encara que deixa fora elements clau com els usuaris i els procediments; és una visió limitada als aspectes tècnics dels sistemes d'informació
- **Sistema de tractament**: és una definició molt circumscrita al Reglament, i simplement atén al nivell d'automatització (ús de tecnologies de la informació i la comunicació) amb què és tractada la informació.
- **Suport**: Fa referència a qualsevol contenidor d'informació en un sentit ampli, per tant es refereix a qualsevol instrument d'emmagatzematge de dades o informació de caràcter personal.
- **Transmissió de documents**: és una definició que tampoc necessita massa explicació. Recull tots els supòsits de transmissió de la informació (moure la informació d'una ubicació a una altra), amb independència del seu suport o tractament
- **Usuari**: qualsevol persona o procés que accedeix a dades personals

La seguretat i el factor humà

Tal com preveu l'article 88 del RLOPD les mesures tècniques i organitzatives que hagin de ser aplicades pel responsable del tractament són d'obligat compliment per al personal amb accés als sistemes d'informació.

Per tant, el factor humà és bàsic per a un correcte funcionament de les mesures de seguretat, i és per això que el Reglament preveu tota una sèrie de mesures directament relacionades amb les persones, tot i que, de fet, en gairebé totes les mesures de seguretat intervenen persones.

Mesures de nivell bàsic

- *Per a tots els tractaments*
  - **Funcions i obligacions del personal** (articles 89 i 105.2): les funcions i obligacions dels usuaris amb accés a dades personals estaran recollides en el document de seguretat, i és obligació del responsable del fitxer o tractament que el personal amb accés a dades conegui totes i cadascuna de les normes de seguretat que afecten el desenvolupament de les seves funcions, així com les conseqüències en cas d'incompliment.
- *Per als tractaments no automatitzats*
  - **Custòdia dels documents per part del personal** (article 108): quan la documentació en paper sigui fora del llocs destinats al seu emmagatzemament o arxiu, habitualment perquè s'està utilitzant, la persona que estigui a càrrec d'aquests documents ha d'impedir, en tot moment, que persones no autoritzades tinguin accés a la documentació

Mesures de nivell mitjà

- *Per als tractaments automatitzats*
  - **Control d'accés físic** (article 99): només les persones autoritzades en el document de seguretat poden accedir físicament als espais on es trobin instal·lats els equipaments físics que donen suport als sistemes d'informació.

Protegint l'accés a les dades

Ja hem esmentat que una de les exigències del principi de seguretat és evitar l'accés a les dades i evitar els tractaments no autoritzats. Per tant, el Reglament obliga a implantar mesures de seguretat que tenen per objectiu evitar els accessos i tractaments no autoritzats.

Mesures de nivell bàsic

- *Per a tots els tractaments*
  - **Control d'accés** (articles 91 i 105.2): cada usuari ha d'estar autoritzat només a accedir a aquella informació necessària per al desenvolupament de les seves funcions, per tant ha d'existir una relació, sempre actualitzada, dels usuaris i dels accessos autoritzats. S'han d'establir controls per evitar que es produeixin accessos a informació personal per part d'usuaris no autoritzats. Aquestes mesures de seguretat afecten tant a personal propi com extern.
- *Per als tractaments automatitzats*
  - **Identificació i autenticació** (article 93): el responsable del fitxer o tractament ha d'establir els mecanismes necessaris per garantir la identificació i autenticació inequívoca i personalitzada dels usuaris (veure definicions a l'apartat 7.3.1). Les contrasenyes s'han de proporcionar i emmagatzemar de manera que quedi garantida la seva confidencialitat i integritat; amb una periodicitat no superior a un any les contrasenyes han de ser modificades.
- *Per als tractaments no automatitzats*
  - **Dificultar l'accés al dispositiu que conté documents** (article 107): l'accés als arxius, armaris, calaixos, etc. on es guardin documents s'ha de realitzar mitjançant algun mecanisme que obstaculitzi el lliure accés (panys o similars)
  - **Evitar l'accés a persones no autoritzades** (article 107): si per les característiques de lloc on s'emmagatzemen els documents no és possible implantar mecanismes que obstaculitzin el lliure accés (prestatgeries per exemple), el responsable del tractament ha d'adoptar altres mesures que impedeixin l'accés de persones no autoritzades.

Mesures de nivell mitjà

- *Per als tractaments automatitzats*
  - **Limitació dels intents d'accés no autoritzat** (article 98): ha d'existir un mecanisme que impedeixi que es puguin intentar reiteradament accessos no autoritzats a un sistema d'informació (per exemple, preveure un nombre màxim d'errors en introduir la contrasenya)

Mesures de nivell alt

- *Per a tots els tractaments*
  - **Registre d'accessos a la informació o documentació** (articles 103 i 113): quan es tracta de dades especialment protegides s'exigeix que es registri l'activitat dels usuaris (què fan amb les dades). D'aquesta manera, cada vegada que un usuari intenta accedir a les dades personals s'ha d'enregistrar la identificació de l'usuari, la data i hora de l'intent d'accés, el fitxer sobre el qual s'intenta l'accés, el tipus d'accés (consulta o modificació) i si l'accés és denegat o autoritzat pel sistema de control d'accés. En aquells casos en què l'accés hagi estat autoritzat, també s'ha de guardar informació que permeti identificar a quines dades es va accedir.
    Els mecanismes de registre d'accés no poden ser desactivats, ni tampoc manipulada la informació que recullen. Aquesta informació s'ha de conservar durant dos anys i com a mínim cada mes el responsable de seguretat ha de revisar aquesta informació i fer un informe.

Si el responsable del fitxer o tractament és una persona física i garanteix que únicament ell pot accedir i tractar les dades, llavors no és necessari que implanti aquesta mesura de seguretat.
En cas de documents en paper s'ha de registrar la informació de quins usuaris han accedit a la documentació.

- *Per als tractaments automatitzats*
  - **Xifratge de les telecomunicacions** (article 104): quan es transmetin dades de nivell alt per xarxes públiques de telecomunicacions o xarxes sense fils de comunicacions electròniques, la informació ha d'anar xifrada o s'ha d'implantar qualsevol mecanisme que faci inintel·ligible la informació i n'impedeixi la manipulació.
- *Per als tractaments no automatitzats*
  - **Dispositius d'emmagatzemament en zones tancades** (article 111): els armaris, arxivadors i dispositius en el quals s'emmagatzemi la informació han d'estar ubicats en àrees protegides mitjançant portes d'accés que restaran tancades i que incorporaran dispositius de tancament, com ara claus o altres mecanismes, que impedeixin el lliure accés a les sales. Si els locals no permeten implantar aquesta mesura, el responsable del fitxer o tractament ha d'adoptar mesures alternatives que han d'estar motivades i descrites en el document de seguretat.
  - **Control de la còpia o reproducció dels documents** (article 112.1): qualsevol còpia o reproducció d'un document en paper només podrà ser realitzada sota el control del personal autoritzat en el document de seguretat.

Salvaguarda i custòdia de la informació

La informació que gestionen els sistemes d'informació pot estar ubicada en diferents llocs. Quan es tracta de tractaments automatitzats, habitualment ens trobem amb dos tipus d'ubicacions: l'emmagatzemament relacionat amb els sistemes d'informació d'explotació normal de les dades i l'emmagatzemament en dispositius externs, ja sigui amb la finalitat de disposar de còpies de seguretat de la informació o per al seu transport i posterior descàrrega en altres sistemes d'informació o dispositius d'explotació de dades. Si es tracta de documents en paper, també ens podem trobar amb les ubicacions relacionades amb la gestió i tramitació ordinària de la documentació i les situacions d'arxiu de la documentació.

En tots els casos, la informació sempre ha d'estar protegida per donar resposta tant al requeriment d'evitar l'accés o tractament no autoritzat, com al d'evitar l'alteració descontrolada de la informació o la pèrdua de les dades.

Mesures de nivell bàsic

- *Per a tots els tractaments*
  - **Gestió de suports i documents** (articles 92 i 105.2): tant els suports digitals d'informació com els documents que continguin dades de caràcter personal han de permetre identificar quin tipus d'informació contenen: els suports informàtics han de poder ser inventariats i només poden accedir a aquests suports les persones autoritzades.
    Qualsevol sortida d'informació fora dels locals habituals de tractament de les dades ha de ser autoritzada pel responsable de fitxer o tractament, i això inclou les trameses per correu electrònic.
    El transport de suports i documentació s'ha de fer amb mesures que impedeixin la sostracció, la pèrdua o l'accés no autoritzat als dispositius i documents.
    Si un suport o document ha de ser destruït, s'han de prendre mesures a fi que la informació no pugui ser recuperada posteriorment.
- *Per als tractaments automatitzats*

  - **Còpies de suport i recuperació** (article 94): s'han de fer còpies de seguretat com a mínim setmanalment, i cada sis mesos el responsable del fitxer o tractament ha de verificar que els procediments de còpia i restauració funcionen correctament.

- *Per als tractaments no automatitzats*
  - **Arxiu. Garantir la conservació** (article 106): l'arxiu de documents es farà segons el que estableixi la legislació específica, però en tot cas s'ha de garantir que la informació es conserva en correctes condicions.
  - **Arxiu. Localització i consulta** (article 106): el sistema d'arxiu ha de facilitar la localització i consulta de la documentació.
  - **Arxiu. Exercici de drets** (article 106): en cap cas el sistema d'arxiu ha de ser obstacle perquè les persones afectades puguin exercir els drets d'accés, rectificació, cancel·lació i oposició en les condiciones previstes a la legislació.

Mesures de nivell alt

- *Per a tots els tractaments*
  - **Xifratge de suports durant el transport i protecció de la documentació** (articles 101 i 114): el reglament ordena prendre certes cauteles durant el transport de suports amb informació o documentació. En cas dels suports, les dades han d'anar xifrades, o bé s'han d'utilitzar mecanismes alternatius que impedeixin l'accés o la manipulació de la informació durant el transport (això s'aplica tant als suports com als documents en paper).
- *Per als tractaments automatitzats*
  - **Identificació de suports codificada** (article 101.1): els suports que continguin dades personals de nivell alt s'han d'etiquetar de manera que només les persones autoritzades coneguin el tipus d'informació continguda en el suport.
  - **Xifratge de dispositius portàtils** (article 101.2): si la informació és en ordinadors portàtils, fora dels locals habituals de tractament, la informació també haurà de ser xifrada. S'ha d'evitar el tractament de dades sensibles en dispositius portàtils que no puguin ser xifrats.
- *Per als tractaments no automatitzats*
  - **Destrucció de les còpies sense utilitat** (article 112.2): un cop les còpies de documents deixen de ser útils han de ser destruïdes, de manera que s'eviti l'accés a la informació que contenien o que aquesta informació pugui ser recuperada (això implica la utilització de destructores de paper o procediments amb resultats similars).

Gestió dels incidents

Les mesures de seguretat no sempre poden evitar que es produeixin incidents amb la informació, per tant, com a mesura que pot evitar futurs incidents de les mateixes característiques, la legislació obliga a portar un registre i a documentar els incidents en què es puguin veure afectades dades de caràcter personal.

Mesures de nivell bàsic

- *Per a tots els tractaments*
  - **Registre d'incidències** (articles 90 i 105.2): el responsable del fitxer o tractament ha de preveure sempre un procediment per comunicar les incidències i ha de crear un registre on consti el tipus d'incident, quan s'ha produït o detectat, la persona que ha notificat l'incident, qui ha rebut la comunicació, quines actuacions s'han dut a terme i quines mesures correctores s'han implantat a fi de que no torni a succeir el mateix incident.

Mesures de nivell mitjà

- *Per als tractaments automatitzats*
  - **Registrar els procediments de recuperació com a incidents** (article 100): a banda de les informacions que preveu l'article 90, quan es tracti de dades que requereixen mesures de seguretat de nivell mitjà, el registre d'incidències també ha d'incloure informació sobre els procediments de restauració que hagin estat necessaris realitzar amb motiu d'un incident. En aquests supòsits s'ha d'indicar quina persona ha realitzat el procés de restauració de les dades, quines dades s'han recuperat i, si es dóna el cas, si s'han recuperat dades manualment.

Mesures organitzatives

La seguretat no és exclusivament una qüestió de tecnologia o dispositius mecànics; algunes mesures són exclusivament de caràcter organitzatiu. La combinació de tots dos tipus de mesures, tècniques i organitzatives, és el que millor garanteix un alt grau d'eficàcia en la protecció de la informació.

Mesures de nivell mitjà

- *Per a tots els tractaments*
  - **Responsable de seguretat** (articles 95 i 109): el document de seguretat conté la designació del responsable de seguretat, que és qui coordina i controla les mesures de seguretat previstes. Aquesta designació en cap cas suposa cap rebaixa en la responsabilitat dels responsables de fitxers o tractaments o dels encarregats de tractament.
  - **Auditoria** (articles 96 i 110): cada dos anys, com a mínim, s'ha de verificar mitjançant una auditoria, que pot ser interna o externa, si les mesures de seguretat previstes funcionen correctament. Si hi ha canvis substancials en els sistemes d'informació, s'ha de fer aquesta auditoria abans del termini de dos anys.
    Com a conseqüència de l'auditoria, s'ha de redactar un informe on es dictamini sobre el grau d'adequació de les mesures previstes al que estableix la legislació, identificar les possibles deficiències trobades i proposar les mesures correctores necessàries.
    És important tenir en compte que els informes d'auditoria han de ser revisats pel responsable de seguretat, el qual ha informar sobre les conclusions al responsable del fitxer o tractament afectat per l'auditoria. Aquests informes d'auditoria han de quedar a disposició de les autoritats de control competents (agencies de protecció de dades).
  - **Registre d'entrada i sortida de suports** (articles 97 i 105): ha d'existir un registre d'entrada i sortida de suports i documents, el qual ha de permetre conèixer el tipus de suport o document que ha entrat o sortit, juntament amb la data i hora, qui és el remitent, el número de documents o suports, el tipus d'informació que contenen, el mecanisme de tramesa i qui ha estat la persona responsable de la recepció.

Mesures de nivell alt

- *Per als tractaments automatitzats*
  - **Evitar concurrència de riscos en còpies i procediments de recuperació** (article 102): el Reglament obliga que les còpies de seguretat i els procediments de recuperació es conservin en un lloc diferent als equipaments informàtics que contenen les dades, és a dir, que no estiguin sota les mateixes amenaces físiques. Evidentment, en aquesta ubicació diferenciada s'han de prendre totes les mesures de seguretat que siguin d'aplicació.

Supòsits especials

El reglament regula algunes situacions molt concretes relacionades amb els tractaments de dades personals, que completen les obligacions dels responsables de fitxers i tractaments en matèria de seguretat i protecció de dades.

1. **Prestacions de serveis sense accés a dades** (article 83): el responsable del fitxer o tractament ha d'adoptar mesures que afectaran a persones que en principi no han d'accedir a dades personals, però que en el desenvolupament normal de les seves funcions poden estar en disposició d'accedir-hi (personal de manteniment, neteja, vigilància, etc.). Com a principi general s'ha de limitar, en la mesura del possible, l'accés a la informació i, en el cas de personal extern, en els contractes s'haurà de fer constar expressament la prohibició d'accés a dades personals i, en tot cas, l'obligació de guardar secret.
2. **Accés mitjançat xarxes de comunicacions** (article 85): quan es transmetin dades personals utilitzant xarxes de comunicacions, siguin públiques o no, s'ha de garantir un nivell de protecció equivalent al previst per als accessos en local.
3. **Treball fora dels locals o ubicacions habituals de tractament** (article 86): per emmagatzemar les dades personals en dispositius portàtils o per tractar-les fora dels locals habituals del responsable del fitxer o tractament, o si s'escau, de l'encarregat del tractament, serà necessària l'autorització prèvia del responsable del fitxer o tractament, i òbviament s'haurà de garantir el nivell de seguretat exigit pel Reglament.
4. **Fitxers de treball i còpies de treball de documents** (article 87): els fitxers temporals o còpies de treball han d'estar protegides segons el nivell de mesures de seguretat que siguin d'aplicació a les dades que continguin i hauran de ser esborrats o destruïts una vegada deixin de ser útils per a les finalitats que van motivar la seva creació.

Unitat 8: Codis tipus

Concepte

Els codis tipus es poden definir com un manual de bones pràctiques o codi deontològic mitjançant el qual una determinada entitat o grup d'entitats delimita les condicions d'organització, règim de funcionament, procediments aplicables, normes de seguretat de l'entorn, programes o equips, obligacions dels implicats en el tractament i ús de la informació personal, així com les garanties, en el seu àmbit, per a l'exercici dels drets de les persones, sempre partint del compliment d'allò que s'estableix a la normativa de protecció de dades personals.

Els codis tipus són voluntaris però són vinculants per als qui s'hi adhereixen.

Els codis tipus es poden referir a un sector i, si és així, poden ser d'aplicació a la totalitat o a una part dels tractaments portats a terme per les entitats que pertanyen al sector de referència. En aquest cas, han de ser formulats per les organitzacions representatives del sector esmentat, almenys en el seu àmbit territorial d'aplicació.

També poden ser promoguts per una empresa o Administració pública i, en aquest cas, s'han de referir a la totalitat dels tractaments que porta a terme l'entitat.

Contingut dels codis tipus

Als articles 73 i 74 del RLOPD s'estableix el contingut dels codis tipus. S'hi indica que han d'estar redactats en termes clars i accessibles i que, com a mínim, han de contenir:

a) La delimitació clara i precisa del seu àmbit d'aplicació, les activitats a què el codi es refereix i els tractaments que hi estan sotmesos.

b) Les previsions específiques per a l'aplicació dels principis de protecció de dades.

c) L'establiment d'estàndards homogenis per al compliment per part dels adherits al codi de les obligacions que estableix la Llei orgànica 15/1999, de 13 de desembre.

d) L'establiment de procediments que facilitin als afectats l'exercici dels seus drets d'accés, rectificació, cancel·lació i oposició.

e) La determinació de les cessions i transferències internacionals de dades que, si s'escau, es prevegin, amb indicació de les garanties que s'hagin d'adoptar.

f) Les accions formatives en matèria de protecció de dades dirigides als qui les tractin, especialment quant a la seva relació amb els afectats.

g) Els mecanismes i procediments de supervisió independents que serveixin per assegurar el compliment de les obligacions assumides pels adherits, i establir un règim sancionador adequat, eficaç i dissuasiu.

h) Clàusules tipus per a l'obtenció del consentiment dels afectats per al tractament o la cessió de les seves dades.

i) Clàusules tipus per informar els afectats del tractament, quan les dades no s'obtinguin dels mateixos afectats.

j) Models perquè els afectats exerceixin els seus drets d'accés, rectificació, cancel·lació i oposició.

k) Models de clàusules per al compliment dels requisits formals exigibles per a la contractació d'un encarregat del tractament, si s'escau.

D'altra banda, es poden afegir compromisos addicionals que afavoreixin el compliment de la normativa de protecció de dades personals i, per exemple, es pot fer referència a:

a) L'adopció de mesures de seguretat addicionals a les que exigeix la normativa de protecció de dades personals.

b) La identificació de les categories de cessionaris o importadors de les dades.

c) Les mesures concretes adoptades en matèria de protecció dels menors o de determinats col·lectius d'afectats.

d) L'establiment d'un segell de qualitat que identifiqui els adherits al codi.

Procediment de supervisió

Els mecanismes i procediments de supervisió que s'estableixin per assegurar el compliment de les obligacions assumides pels adherits, han de garantir:

a) La independència i imparcialitat de l'òrgan responsable de la supervisió.

b) La senzillesa, accessibilitat, celeritat i gratuïtat per a la presentació de queixes i reclamacions davant l'òrgan esmentat pels eventuals incompliments del codi tipus.

c) El principi de contradicció.

d) Una graduació de sancions que permeti ajustar-les a la gravetat de l'incompliment. Aquestes sancions han de ser dissuasives i poden implicar la suspensió de l'adhesió al codi o l'expulsió de l'entitat adherida. Així mateix, pot establir-se, si s'escau, la seva publicitat.

e) La notificació a l'afectat de la decisió adoptada.

Finalment, si es considera pertinent, els codis tipus poden preveure procediments per tal de determinar mesures reparadores en cas que s'hagi causat un perjudici als afectats com a conseqüència de l'incompliment del codi tipus.

El codi tipus ha d'incorporar, com a annex, una relació d'adherits que s'ha de mantenir actualitzada i a disposició de l'Agència de Protecció de Dades.

Inscripció en el Registre de Protecció de Dades de Catalunya

L'article 15 de la Llei 5/2002, de 19 d'abril, de creació de l'Agència Catalana de protecció de Dades, estableix que els codis tipus formulats per la Generalitat de Catalunya o pels ens que integren l'Administració local en l'àmbit territorial de Catalunya han de ser inscrits en el Registre de Protecció de Dades de Catalunya.

Hem de tenir en compte que l'àmbit competencial de l'Agència Catalana de Protecció de Dades ha variat a partir de l'establert a l'article 156 de l'Estatut d'Autonomia de Catalunya i, per tant, hem d'aplicar, respecte de l'obligació d'inscriure els codis tipus a l'Agència Catalana, el mateix criteri que respecte de la inscripció de fitxers i atenir-nos a l'establert en l'esmentat article.

En tot cas, el Registre pot denegar-ne la inscripció quan consideri que no s'ajusta a les disposicions legals i reglamentàries sobre la matèria, i, en aquest cas, el director de l'Agència de Protecció de Dades ha de requerir els sol·licitants perquè facin les correccions oportunes.

Obligacions posteriors a la inscripció del codi tipus

Les entitats promotores o els òrgans, les persones o les entitats que a aquest efecte es designin en el mateix codi tipus tenen, una vegada hagi estat publicat, les obligacions següents:

a) Mantenir accessible al públic la informació actualitzada sobre les entitats promotores, el contingut del codi tipus, els procediments d'adhesió i de garantia del seu compliment i la relació d'adherits a què es refereix l'article anterior.

Aquesta informació s'ha de presentar de forma concisa i clara i ha d'estar permanentment accessible per mitjans electrònics.

b) Remetre a l'Agència Catalana de Protecció de Dades una memòria anual sobre les activitats realitzades per difondre el codi tipus i promoure-hi l'adhesió, les actuacions de verificació del compliment del codi i els seus resultats, les queixes i reclamacions tramitades i el curs que se'ls ha donat, i qualsevol altre aspecte que les entitats promotores considerin adequat destacar.

c) Avaluar periòdicament l'eficàcia del codi tipus mesurant el grau de satisfacció dels afectats i, si s'escau, actualitzar-ne el contingut per adaptar-lo a la normativa general o sectorial de protecció de dades existent en cada moment.

Aquesta avaluació ha de tenir lloc almenys cada quatre anys, llevat que sigui necessari adaptar els compromisos del codi a la modificació de la normativa aplicable en un termini més curt.

d) Afavorir l'accessibilitat de totes les persones, amb una especial atenció a les que tinguin alguna discapacitat o edat avançada, a tota la informació disponible sobre el codi tipus.