Intimitat i dades personals a Internet

Mònica Vilasau Solana
Maria Àngels Vila Muntal

PID_00162527

UOC
Universitat Oberta de Catalunya
www.uoc.edu

Cap part d'aquesta publicació, incloent-hi el disseny general i la coberta, no pot ser copiada, reproduïda, emmagatzemada o transmesa de cap manera ni per cap mitjà, tant si és elèctric com químic, mecànic, òptic, de gravació, de fotocòpia o per altres mètodes, sense l'autorització prèvia per escrit dels titulars del copyright.

Índex

Introducció..... 5

Objectius..... 6

1. Les tecnologies de la informació i comunicació i els reptes per a la vida privada..... 7

2. Evolució normativa sobre la protecció de dades..... 10
2.1. Marc internacional 10
2.2. La regulació vigent a l'Estat espanyol 12
2.2.1. Regulació estatal 12
2.2.2. Regulació autonòmica 13
2.2.3. Configuració del dret fonamental a la protecció de dades a l'Estat espanyol 14

3. La Llei orgànica 15/1999, de protecció de dades de caràcter personal (LOPD)..... 17
3.1. Àmbit d'aplicació 17
3.1.1. El terme *dada*..... 17
3.1.2. El terme *personal*..... 19
3.1.3. Fitxer o tractament de dades 23
3.1.4. Tractaments regulats per la LOPD 23
3.2. Obligacions prèvies al tractament de les dades: creació, modificació i supressió de fitxers 24
3.2.1. Creació, modificació i supressió de fitxers de titularitat pública 24
3.2.2. Creació, modificació i supressió de fitxers de titularitat privada 25
3.2.3. Notificació de fitxers al Registre General de Protecció de Dades 26
3.3. Legitimació per al tractament de les dades de caràcter personal 26
3.3.1. El consentiment de la persona interessada 27
3.3.2. Dades subjectes a una normativa específica 32
3.3.3. El consentiment per al tractament de les dades dels menors 32
3.3.4. Dades procedents de fonts accessibles al públic 33
3.3.5. L'existència d'un interès legítim i el compliment d'una obligació legal 36
3.4. L'obtenció de les dades a partir d'un subjecte diferent de la persona interessada 37

3.4.1. Accessos que es consideren cessió de dades 37
3.4.2. Comunicació de dades entre administracions públiques 39
3.4.3. Accessos que no es consideren cessió de dades: l'encàrrec de tractament 39
3.5. Seguretat i confidencialitat en el tractament de les dades 40
3.5.1. El deure de seguretat en el tractament de les dades de caràcter personal 40
3.5.2. El deure de secret 42
3.6. La regulació de determinats fitxers 42
3.6.1. Els fitxers de les forces i dels cossos de seguretat 42
3.6.2. Els fitxers de solvència patrimonial i crèdit 42
3.6.3. Els fitxers de publicitat i prospecció comercial 44
3.6.4. Els fitxers comuns de les entitats asseguradores 46
3.6.5. Els fitxers de videovigilància 47
3.7. Exercici dels drets d'accés, rectificació, cancel·lació i oposició (ARCO) per la persona afectada 49
3.7.1. Disposicions generals 49
3.7.2. Dret d'accés a les dades 51
3.7.3. Dret de rectificació i cancel·lació 52
3.7.4. El dret d'oposició 53
3.7.5. Reclamació de tutela de drets 53
3.8. Transferència internacional de dades 54
3.9. Responsabilitat administrativa i responsabilitat civil 58
3.9.1. La responsabilitat administrativa 58
3.9.2. La responsabilitat civil 60

Bibliografia..... 63

Introducció

Un dels drets fonamentals reconeguts en la majoria de les cartes de drets fonamentals i en la majoria de les constitucions és el de la intimitat. Un dret a què difícilment volem renunciar en la mesura que ens permet ser més nosaltres mateixos. Tanmateix, les noves tecnologies ens permeten transgredir fronteres noves, conèixer informació que abans era impensable i, sobretot, relacionar, emmagatzemar, buscar i transmetre aquesta informació. Això fa que els senyals d'alerta es disparin, ja que no ens agrada sentir-nos vigilats o retratats, que algú sàpiga de nosaltres més que nosaltres mateixos...

El subjecte, la persona, es converteix en dada, en un conjunt d'informació que pot arribar a ser molt preada, tant per a l'Estat, per al poder, com per als agents econòmics. Fins on podem tolerar les intromissions? Fins on podem posar barreres? És evident que si volem viure en societat, i en una societat informatitzada, hem de fer un cert nombre de renúncies, però quin és l'àmbit indisponible?

Objectius

L'estudi d'aquest mòdul us permetrà assolir els objectius següents:

1. Conèixer quins són els trets que permeten definir el dret a la protecció de dades com un dret fonamental i autònom respecte al dret a la intimitat.

2. Tenir clar el marc normatiu que regula el dret a la protecció de dades.

3. Saber i entendre quins són els principis informadors de la LOPD i del reglament que la desplega.

4. Aprendre quins són els drets que reconeix la LOPD a les persones afectades o interessades i també les seves garanties.

5. Aprendre a quins tractaments de dades resulta aplicable la LOPD i també els requisits que s'estableixen per a tractar les denominades *dades sensibles*.

6. Distingir entre els supòsits en els quals fa falta el consentiment per a l'obtenció i per al tractament de les dades i quan no és necessari. Les diferències entre *revocació del consentiment* i *oposició al tractament*.

7. Conèixer i distingir entre els diferents tipus d'arxius que hi ha i també els requisits per a crear-los, modificar-los i cancel·lar-los.

8. Saber què s'entén per *moviment internacional de dades* i la regulació que duu a terme la LOPD.

9. Conèixer el règim de responsabilitat al qual estan sotmesos la persona responsable i l'encarregada del tractament.

1. Les tecnologies de la informació i comunicació i els reptes per a la vida privada

El dret a la intimitat es troba reconegut en la gran majoria de constitucions i cartes de drets fonamentals. Les tecnologies de la informació i de la comunicació (TIC) tenen una incidència indiscutible en aquest àmbit, ja que obren les portes a informació a la qual abans era impensable accedir, i sobretot permeten buscar, relacionar, emmagatzemar, i transmetre aquesta informació. Tot això ofereix avantatges indubtables; tanmateix, també els senyals d'alerta es disparen davant dels perills que comporten aquestes tecnologies per a la vida privada. Amb les tecnologies digitals la persona es converteix en una dada, en un conjunt d'informació. L'ADN, la imatge, la veu o bé la pràctica totalitat de la vida diària d'un subjecte (pagar amb targetes de crèdit, parlar per telèfon, comprar per Internet, connectar-se a la TV digital, utilitzar un GPS) es pot convertir en bits, en informació digital. Així mateix s'ha de tenir en compte que la navegació per la Xarxa és susceptible de deixar un rastre vinculat a l'adreça IP (pàgines consultades, música descarregada, xats mantinguts).

Si unim aquesta traçabilitat de la informació amb la velocitat creixent dels processadors, la utilització de potents motors de cerca i de relació de dades, obtenim com a resultat que l'individu es converteix en un ésser transparent i el dret a l'oblit queda pràcticament anul·lat. Partint de tota la informació digital es construeixen perfils dels subjectes, es parametritzen els comportaments i s'envia publicitat personalitzada.

En la nostra societat la tecnologia és cada vegada més omnipresent i proliferen els instruments que permeten dur a terme un seguiment més intensiu de l'individu. Entre aquests instruments es pot destacar el GPS, la generalització de les càmeres de videovigilància, els telèfons mòbils –que permeten localitzar els seus usuaris–, la inserció d'etiquetes RFID (identificació per radiofreqüència) en els objectes, o bé els espais d'intel·ligència ambiental. Així mateix la tecnologia assoleix tal nivell de sofisticació que amb freqüència passa desapercebuda, de manera que resulta difícil adonar-se que es deixa un rastre digital.

D'altra banda, la frontera entre l'esfera pública i la privada es va diluint en la mesura que el seguiment descrit es pot fer fins i tot al propi domicili. Les parets físiques ja no constitueixen un obstacle per a conèixer els programes de televisió seguits, el consum d'electricitat, la premsa en línia consultada o bé les aficions i adquisicions per mitjà de la Xarxa. Fins i tot en els àmbits de lleure i d'amistat s'ha estès l'ús de les TIC, i això constitueix l'exemple més paradigmàtic de la generalització de les xarxes socials.

Aquest escenari, en contínua evolució, planteja nombrosos reptes per al dret i per al legislador. Un d'aquests reptes és com queda afectat el dret a la vida privada i com el podem protegir adequadament.

El dret a la vida privada, i més concretament el dret a la intimitat, ha estat configurat com un dret fonamental que deriva de la dignitat de la persona i comporta l'existència d'un àmbit propi i reservat davant l'acció i el coneixement dels altres. En conseqüència, el titular del dret té el poder de protegir aquest àmbit reservat davant el coneixement i la divulgació per a tercers.

Tanmateix, davant de les noves formes d'intromissió en la vida privada, s'han d'establir nous mecanismes de protecció. No n'hi ha prou simplement de posar barreres, sinó que cal proporcionar a l'individu nous instruments perquè pugui controlar activament la seva vida privada i especialment la informació que es genera en relació amb la seva persona. A més, s'ha de tenir en compte que, de vegades, la informació recopilada no pertany estrictament a l'òrbita privada, sinó que pot ser fins i tot de coneixement general, per la qual cosa no quedaria protegida pel dret a la intimitat en sentit estricte. De fet, moltes de les dades poden semblar irrellevants, i algunes ni tan sols s'amaguen. Tanmateix, una informació poc transcendent, si entra dins d'un engranatge i s'acumula amb una altra informació, pot acabar adquirint un gran valor.

Per tant, més que el dret a ocultar, es tracta d'atorgar a l'individu el control de la informació. En l'escenari de la societat de la informació, i davant de les noves formes d'ingerència descrites, es va anar definint un nou dret, el dret a l'autodeterminació informativa o a la protecció de dades de caràcter personal.

La configuració d'aquest dret va quedar clarament perfilada en la Sentència del Tribunal Constitucional alemany de 15 de desembre de 1983, sobre la Llei del cens que va definir el dret a l'autodeterminació informativa com a corol·lari del dret a l'autodeterminació de la persona. Aquest dret comporta que l'individu pugui decidir bàsicament per si mateix quan i dins de quins límits es poden revelar situacions relacionades amb la seva vida. Segons el Tribunal alemany, el desenvolupament lliure de la personalitat pressuposa, en les condicions modernes de l'elaboració de dades, la protecció de l'individu contra la recollida, l'emmagatzemament, la utilització i la transmissió il·limitats de les dades referents a la persona.

Lectura recomanada

La Sentència del Tribunal Constitucional alemany de 15 de desembre de 1983 es pot trobar traduïda al castellà en el *Butlletí de Jurisprudència Constitucional* (núm. 33, any 1984, pàg. 126 i seg.). Es va presentar un recurs contra la Llei del cens de 25 de març de 1982. Aquest recurs, malgrat reconèixer el dret i el deure de l'Estat d'obtenir informació, plantejava el temor que la informació pogués ser utilitzada eventualment contra els drets dels ciutadans.

Les normes relatives al tractament de les dades de caràcter personal constitueixen un instrument per a salvaguardar la vida privada del subjecte. Tanmateix, a l'hora d'atorgar aquesta protecció, s'ha de ponderar l'existència d'altres drets; especialment la llibertat d'expressió i el dret a comunicar i rebre informació i l'accés a la informació generada pel sector públic.

Així mateix, en la interacció entre els subjectes interessats en l'intercanvi de dades, també s'haurà de tenir en compte el principi de llibertat d'empresa en el marc de l'economia de mercat.

L'entramat i l'equilibri entre els drets implicats va quedar distorsionat per un factor nou: la reivindicació de la seguretat. Com a conseqüència dels greus atemptats terroristes de setembre de 2001, es va plantejar amb més força l'exigència de seguretat. Això va ocasionar un control cada vegada més omnipresent de la vida privada amb una finalitat preventiva. En conseqüència, al costat de les normes relatives a la protecció de dades, s'han anat aprovant normes que cada vegada pretenen un control més ferri de la informació, especialment de la que circula per Internet, per a fer front a les amenaces del terrorisme i del crim organitzat.

Al llarg de les pàgines següents s'exposarà quin és el marc legislatiu de la protecció de dades com a instrument privilegiat per a garantir un espai íntim a la persona. Alguns autors de referència posen de manifest que l'existència d'aquesta esfera, estretament relacionada amb el dret a l'autodeterminació del subjecte i al desenvolupament lliure de la personalitat, no és un dret més entre els altres, sinó el pressupòsit per a l'exercici d'altres drets i fins i tot el fonament d'una societat veritablement democràtica.

2. Evolució normativa sobre la protecció de dades

La preocupació per la protecció de les dades personals ha portat a l'elaboració de diversos instruments normatius, tant des del punt de vista internacional com des del punt de vista del dret intern.

2.1. Marc internacional

Com hem indicat, davant de les amenaces al dret a la intimitat i al tractament il·limitat de les dades personals, el dret ha intentat donar una resposta i salvaguardar els drets fonamentals de la persona ponderant els interessos que hi ha en joc. Aquest impuls s'ha centrat en l'establiment d'una normativa específica per a regular el tractament de les dades personals, l'adopció de mesures relatives al secret de les comunicacions i la creació de les agències de protecció de dades com a autoritats independents amb la missió de controlar el compliment d'aquestes reglamentacions.

Un primer moviment legislatiu es va originar a partir de la primera llei sobre protecció de dades aprovada pel Parlament del *land* alemany de Hessen el 1970. Altres països com Suècia, els Estats Units, Nova Zelanda, el Canadà i gran part dels estats europeus, també es van dotar d'instruments legislatius sobre aquesta matèria.

Legislació sobre protecció de dades als Estats Units

En el cas dels Estats Units, es tracta de normes sectorials, no d'una norma de caràcter general sobre protecció de dades.

Un altre impuls legislatiu a escala internacional es va deure al Conveni 108 del Consell d'Europa, de 28 de gener de 1981, de protecció de les persones amb relació al tractament automatitzat de les dades de caràcter personal.

Lectura recomanada

Una traducció no oficial del Conveni 108 del Consell d'Europa es pot consultar en la pàgina web de l'AEPD, canal de documentació: <https://www.agpd.es>.

Posteriorment, en l'àmbit comunitari es van dictar 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 respecte al tractament de dades personals i a la lliure circulació d'aquestes dades, i la Directiva 2002/58/CE del Parlament Europeu i del Consell, de 12 de juliol de 2002, relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques, modificada per la Directiva 2009/136/CE.

Lectura recomanada

La Directiva 95/46/CE del Parlament Europeu i del Consell va ser publicada en el *Diari Oficial de la Comunitat Europea* (DOCE), L 281, de 23 de novembre de 1995.

També s'ha de tenir en compte la Directiva 2006/24/CE del Parlament Europeu i del Consell, de 15 de març de 2006, sobre la conservació de dades generades o tractades amb relació a la prestació de serveis de comunicacions electròniques d'accés públic o de xarxes públiques de comunicacions, i per la qual es modifica la Directiva 2002/58/CE. La Directiva 2006/24/CE va ser traslladada

a l'ordenament jurídic espanyol per la Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.

Lectura recomanada

La Directiva 2002/58/CE del Parlament Europeu i del Consell va ser publicada en el DOCE, L 105, 13 d'abril de 2006.

L'article 33 de la Directiva 95/46/CE estableix que la Comissió ha de presentar periòdicament al Consell i al Parlament Europeu un informe sobre l'aplicació d'aquesta Directiva, acompanyat de les propostes de modificació que es considerin oportunes. El primer informe es va adoptar el maig de 2003 i, entre altres conclusions, va constatar que la Directiva havia assolit l'objectiu d'atorgar prou protecció a la privacitat, alhora que havia facilitat la transferència de dades en la Unió Europea (UE). Ara bé, la tardança d'alguns estats membres en la implementació de la Directiva i també les diferències en la seva transposició van motivar que l'economia europea no hagués obtingut un benefici complet de la Directiva en qüestió. L'informe va proposar un pla de treball a fi de reduir les diferències, basat en la cooperació entre els estats membres i entre aquests i la Comissió.

Lectura recomanada

La modificació de la Directiva 2002/58/CE es va publicar en el DOCE, L 105, 13 d'abril de 2006.

Enllaç recomanat

Respecte a la implementació de la Directiva 95/46 en els diferents estats membres, podeu consultar: <http://europa.eu.int/comm/justice_home/fsj/privacy/law/implementation_en.htm>.

L'any 2009 la Comissió Europea va adreçar al grup de treball de l'article 29 una consulta sobre l'adequació de la Directiva 95/46/CE a la realitat tecnològica del moment i al fenomen de la globalització, i va plantejar si els canvis tecnològics esdevinguts comportaven la necessitat de modificar el marc legal, concretament aquesta Directiva. El grup de treball de l'article 29 va emetre un informe sobre els aspectes que s'haurien de tenir en compte de cara a una reforma d'aquest text legislatiu. Es tracta del document de treball número 168, d'1 de desembre 2009 (WP 168, *The Future of Privacy*). Aquest document considera que els principis establerts en la Directiva continuen encara vigents, si bé s'han d'implementar en el nou entorn social i tecnològic.

Enllaç recomanat

Aquest WP té l'origen en la consulta que la Comissió Europea va adreçar a aquest grup sobre l'adequació de la normativa de protecció de dades a la realitat tecnològica del moment i al fenomen de la globalització. Vegeu aquest document: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm (disponible el 12/3/2010).

Així mateix, assenyala aspectes que s'han de tenir en compte de cara a aquesta adaptació de la normativa: el reforçament del consentiment del subjecte, l'adopció d'una filosofia de *privacy by design* (la qual cosa exigeix que en el moment de dissenyar les aplicacions informàtiques es tinguin en compte i s'adoptin les solucions més protectores de la privacitat), la introducció de *privacy enhancing technologies* (PET), és a dir, tecnologies que comportin, per defecte, una protecció més gran de la privacitat, el reforçament del paper de les autoritats de protecció de dades, el foment de l'educació i proporcionar informació transparent i adequada a l'usuari.

Finalment, en l'àmbit comunitari també cal destacar la Carta dels drets fonamentals de la Unió Europea, de 7 de desembre de 2000, els articles 7 i 8 de la qual es dediquen, respectivament, al respecte a la vida privada i familiar i a la protecció de dades de caràcter personal. Així mateix s'ha de destacar el Reglament (CE) núm. 45/2001 del Parlament Europeu i del Consell, de 18 de desembre de 2000, relatiu a la protecció de les persones físiques respecte al

tractament de dades personals per part de les institucions i els organismes comunitaris i a la lliure circulació d'aquestes dades. Aquest Reglament estableix el marc legal de protecció de dades en l'àmbit de les institucions europees i disposa la creació del supervisor europeu de protecció de dades, autoritat supervisora independent a escala comunitària. Convé tenir en compte també la Decisió marc 2008/977/JAI del Consell, de 27 de novembre de 2008, relativa a la protecció de dades personals tractades en el marc de la cooperació policial i judicial en matèria penal. Es tracta del primer instrument general relatiu a la protecció de dades en el tercer pilar de la UE.

2.2. La regulació vigent a l'Estat espanyol

En aquest apartat esmentem les normes principals que afecten la protecció de dades, tant d'àmbit estatal com autonòmic.

2.2.1. Regulació estatal

L'article 18.4 CE estableix que "la llei limita l'ús de la informàtica per garantir l'honor i la intimitat personal i familiar de la ciutadania i el ple exercici dels seus drets". A partir d'aquest precepte i en funció de la matèria de què es tracti, hi ha diferents blocs normatius que s'apliquen d'una manera més o menys immediata. A més, com a resultat de la distribució de competències entre l'Estat i les comunitats autònomes, també cal tenir en compte les normes dictades en cadascuna d'aquestes instàncies.

El desplegament de l'article 18.4 CE va tenir lloc mitjançant la Llei orgànica 5/1992, de 29 d'octubre, de regulació del tractament automatitzat de dades de caràcter personal (LORTAD).

LORTAD

Es tracta de la Llei orgànica 5/1992, de 29 d'octubre, de regulació del tractament automatitzat de dades de caràcter personal.

Aquesta Llei va ser derogada per la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD). Així, doncs, un primer bloc normatiu per raó de la matèria és integrat principalment per la LOPD, que constitueix el text bàsic i de caràcter general sobre la protecció de dades, juntament amb el reglament que la desplega, el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (RLOPD).

Així mateix, dins d'aquest bloc també es troben normes específiques, relatives a àmbits concrets que afecten directament les dades de caràcter personal, com les bases de dades d'ADN, les dades referents a la salut i als historials clínics, o bé les dades sobre comunicacions electròniques.

Lectures recomanades

Sobre els codis en general, vegeu l'article 18 LSSI i, respecte al cas concret de la protecció de dades, vegeu els articles 32 LOPD i 71-78 RLOPD.

Lectures recomanades

Entre d'altres, vegeu: la Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i dels drets i obligacions en matèria d'informació i documentació clínica; la Llei 14/2007, de 3 de juliol, de recerca biomèdica; la Llei orgànica 10/2007, de 8 d'octubre, reguladora de la base de dades policial sobre identificadors obtinguts a

partir de l'ADN, i la Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.

Lectures recomanades

Entre d'altres, vegeu: la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (LSSI); la Llei 32/2003, de 3 de novembre, general de telecomunicacions; la Llei 11/2007, de 22 de juny, d'accés electrònic de la ciutadania als serveis públics; la Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic, i la Llei 56/2007, de 28 de desembre, de mesures d'impuls de la societat de la informació.

Un segon bloc normatiu seria integrat per les disposicions relatives al comerç i a l'Administració electrònica.

Al seu torn, dins del context d'Internet i també en matèria de protecció de dades, cal fer referència als elements d'autoregulació que sorgeixen. Es tracta de mecanismes d'autocontrol que normalment ocorren en el sector privat, però que no són exclusius d'aquest àmbit.

Constitueixen un exemple d'aquesta activitat els denominats *codis tipus*, codis de conducta que poden acordar un grup d'empreses o les administracions públiques a fi d'establir una sèrie de regles, unes condicions d'organització, un règim de funcionament, uns procediments aplicables, unes normes de seguretat, uns polítiques en el tractament de les dades personals, etcètera.

Finalment, integren el tercer bloc normatiu les disposicions de caràcter general i de diferent naturalesa que resulten aplicables en funció del seu rang i del bé jurídic protegit.

Exemples de normatives de protecció de dades

Una mostra en seria la Llei orgànica 1/1982, de 5 de maig, de protecció civil dels drets fonamentals a l'honor, a la intimitat personal i familiar i a la pròpia imatge, el Codi civil (CC) o el Codi penal. Aquest últim Codi resulta aplicable com a *ultima ratio* i sanciona les conductes que es consideren més greus.

2.2.2. Regulació autonòmica

Dins del marc regulador de la protecció de dades cal tenir en compte l'existència tant de normes estatals com de normes autonòmiques. L'Agència Espanyola de Protecció de Dades és l'autoritat de control competent de salvaguardar el respecte del dret fonamental a la protecció de dades referent als tractaments de dades efectuades pel sector privat en la seva totalitat, i per una part del sector públic, ja que hi ha algunes autoritats de control autonòmiques amb competències en la matèria. Així, algunes comunitats autònomes, dins del marc competencial que els atorguen la CE, els estatuts d'autonomia i la LOPD, també han dictat les seves pròpies normes.

Agència Espanyola de Protecció de Dades

Obtindreu informació sobre l'Agència Espanyola de Protecció de Dades a http://www.agpd.es. També l'Agència Espanyola de Protecció de Dades s'està adaptant al nou marc que estableix l'Administració electrònica; un exemple recent d'això és la creació de la seva seu electrònica mitjançant la Resolució, de 18 de març de 2010, de l'Agència Espanyola de Protecció de Dades, per la qual es crea la seu electrònica de l'Agència Espanyola de Protecció de Dades (BOE, núm. 72, de 24 de març de 2010).

L'article 41 de la LOPD permet que determinades funcions de l'Agència Espanyola de Protecció de Dades (AEPD), quan afectin fitxers de dades de caràcter personal creats o gestionats per les comunitats autònomes i per l'Administració local, siguin exercides pels òrgans corresponents de cada comunitat, que tenen la consideració d'autoritats de control. D'acord amb aquesta habilitació normativa, algunes comunitats autònomes han dictat normes per crear les agències de protecció de dades respectives i la normativa corresponent que les desplega.

Lectura recomanada

Per a més informació sobre la protecció jurídica de dades de caràcter personal a Catalunya, podeu consultar la Llei orgànica 6/2006, de 19 de juliol, de reforma de l'Estatut d'autonomia de Catalunya, publicada pel Decret 306/2006, de 20 de juliol, pel qual es dóna publicitat a la Llei orgànica 6/2006, de 19 de juliol, de reforma de l'Estatut d'autonomia de Catalunya.

Exemples d'agències autonòmiques de protecció de dades

La primera autoritat de control autonòmica va ser la de la Comunitat de Madrid, creada mitjançant la Llei 13/1995, de 21 d'abril, de regulació de l'ús de la informàtica en el tractament de dades personals per la Comunitat de Madrid. En el cas de la Comunitat Autònoma de Catalunya, el seu Estatut d'autonomia reconeix en l'article 31 el dret a la protecció de dades personals i l'article 156 estableix les competències de la Generalitat en matèria de protecció de dades de caràcter personal. Anteriorment, ja s'havia creat l'Agència Catalana de Protecció de Dades, mitjançant la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades. L'última autoritat de control autonòmica creada va ser la basca, mitjançant la Llei 2/2004, de 25 de febrer, de fitxers de dades de caràcter personal de titularitat pública i de creació de l'Agència Basca de Protecció de Dades.

Les agències autonòmiques tenen encomanada la funció de vetllar pels fitxers de caràcter públic que hi ha en els seus respectius àmbits territorials. Tanmateix i com es veurà més endavant, no sempre és fàcil determinar què s'entén per *fitxer de caràcter públic*.

2.2.3. Configuració del dret fonamental a la protecció de dades a l'Estat espanyol

La LOPD va ser objecte d'un recurs d'inconstitucionalitat estimat parcialment per la STC 292/2000, de 30 de novembre. En aquesta Sentència, el Tribunal Constitucional va posar en relleu que el dret protegit en l'article 18.4 CE és un dret fonamental diferent del dret a la intimitat de l'article 18.1 CE, ja que aquest últim pot resultar insuficient a l'hora de protegir l'individu davant la nova realitat derivada del progrés tecnològic. El fonament jurídic sisè de la Sentència plasma aquesta doctrina:

"La funció del dret fonamental a la intimitat de l'article 18.1 CE és la de protegir davant qualsevol invasió que es pugui fer en aquell àmbit de la vida personal i familiar que la persona vol excloure del coneixement aliè i de les intromissions de tercers en contra de la seva voluntat (per totes STC 144/1999, de 22 de juliol, FJ 8). En canvi, el dret fonamental a la protecció de dades persegueix garantir a aquesta persona un poder de control sobre les seves dades personals, sobre el seu ús i la seva destinació, per tal d'impedir-ne el tràfic il·lícit i lesiu per a la dignitat i dret de la persona afectada. En fi, el dret a la intimitat permet excloure certes dades d'una persona del coneixement aliè; per aquesta raó, i així ho ha dit aquest Tribunal (STC 134/1999, de 15 de juliol, FJ 5; 144/1999, FJ 8; 98/2000, de 10 d'abril, FJ 5; 115/2000, de 10 de maig, FJ 4), és a dir, el poder de protegir la seva vida privada d'una publicitat no volguda. El dret a la protecció de dades garanteix als individus un poder de disposició sobre aquestes dades. Aquesta garantia imposa als poders públics la prohibició que es converteixin en fonts d'aquesta informació sense les garanties degudes; i també el deure de prevenir els riscos que es puguin derivar de l'accés o la divulgació indeguts d'aquesta informació. Però aquest poder de disposició sobre les dades personals pròpies no val res si la persona afectada desconeix quines dades són les que tenen terceres persones, qui les té i amb quina finalitat."

Segons el Tribunal Constitucional, quins són els trets que permeten configurar el dret tutelat en l'article 18.4 CE com un dret autònom respecte al de l'article 18.1 CE? Si el dret a la intimitat (art. 18.1 CE) permet excloure certes dades d'una persona del coneixement aliè, és a dir, atorga al titular el poder de protegir la seva vida privada d'una publicitat no volguda, el dret a la protecció de dades (art. 18.4 CE) garanteix als individus un poder de disposició sobre aquestes dades. Aquests dos drets comparteixen un mateix objectiu: oferir una protecció constitucional eficaç de la vida privada personal i familiar. Tanmateix, també hi ha una sèrie de diferències a causa de la seva funció específica, que es poden concretar des del punt de vista del seu objecte i el seu contingut.

D'una banda, l'objecte de l'article 18.4 CE és més ampli que el dret a la intimitat de l'article 18.1 CE. El dret fonamental a la protecció de dades no es limita a les dades íntimes de la persona, sinó que n'estén la garantia a qualsevol tipus de dades personals, siguin o no íntimes, el coneixement de les quals per terceres persones pugui afectar els drets de la persona. Qualsevol dada de caràcter personal que identifiqui o permeti la identificació de l'individu entra dins de l'àmbit de protecció del dret fonamental a la protecció de dades.

D'altra banda, pel que fa al contingut, això són, les facultats que aquests articles atorguen al titular del dret, l'article 18.1 CE confereix a aquest titular el poder jurídic d'imposar a terceres persones el deure d'abstenir-se de tota intromissió en l'esfera íntima de la persona i la prohibició de fer ús del que mitjançant una intromissió hagi estat conegut.

En canvi, el dret a la protecció de dades atribueix a aquest titular un conjunt de facultats que consisteix en diversos poders jurídics l'exercici dels quals imposa deures jurídics a terceres persones. D'aquesta manera, es garanteix a la persona un vertader poder de control sobre les seves dades personals que només és possible i efectiu imposant a terceres persones una sèrie d'obligacions: requerir el consentiment previ per a la recollida de dades personals, informar sobre la destinació i l'ús de les dades recollides, garantir l'accés a les dades, rectificar i cancel·lar les dades quan sigui necessari, etcètera.

> En definitiva, el contingut del dret fonamental a la protecció de dades consisteix en un poder de disposició i de control sobre les dades personals que faculta la persona per decidir quines dades proporciona a una tercera persona, sigui l'Estat o un particular, o quines pot obtenir aquesta tercera persona.

Aquest dret també permet a l'individu conèixer qui té aquestes dades personals, conèixer amb quina finalitat les té i oposar-se a aquesta possessió o ús. Aquests poders de disposició i control sobre les dades personals, que constitueixen part del contingut del dret fonamental a la protecció de dades, es concreten jurídicament en la facultat de consentir la recollida, l'obtenció i l'accés

a les dades personals: el seu emmagatzematge i tractament posteriors, i també el seu possible ús per part d'una tercera persona, sigui l'Estat o un particular. I aquest dret a consentir el coneixement i el tractament, informàtic o no, de les dades personals, requereix, com a complements indispensables, d'una banda, la facultat de saber en tot moment qui disposa d'aquestes dades personals i a quin ús les sotmet i, de l'altra, el fet de poder-se oposar a aquesta possessió i a aquests usos (STC 292/2000, FJ 7).

3. La Llei orgànica 15/1999, de protecció de dades de caràcter personal (LOPD)

La Llei orgànica 15/1999 de protecció de dades de caràcter personal (LOPD) constitueix la principal norma reguladora del dret a la protecció de dades en el nostre ordenament.

3.1. Àmbit d'aplicació

L'article 2.1 de la LOPD, que regula l'àmbit d'aplicació, estableix que "aquesta Llei orgànica és aplicable a les dades de caràcter personal registrades en suport físic, que les faci susceptibles de tractament, i a tota modalitat d'ús posterior d'aquestes dades pels sectors públic i privat". Per tant, l'àmbit d'aplicació es delimita pel concepte de *dada personal* i per la possibilitat del seu tractament.

3.1.1. El terme *dada*

La LOPD estableix que una dada personal és "qualsevol informació relativa a persones físiques identificades o identificables". El RLOPD complementa la definició anterior i entén per *dada de caràcter personal* "qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus relativa a persones físiques identificades o identificables".

El concepte de *dada de caràcter personal* no es limita a la informació numèrica o alfabètica relativa a una persona, sinó que en comprèn també la imatge, la veu, les empremtes dactilars, les denominades *dades biomètriques*, la informació genètica, un text, etcètera, sempre que sigui possible relacionar-los amb una persona concreta. Els criteris interpretatius de les diferents autoritats de control i la jurisprudència han configurat aquest concepte, encara que de vegades no és fàcil concretar si es tracta d'una dada d'aquesta naturalesa, ja que hi ha algunes zones grises. Així, a títol d'exemple, s'ha considerat dada de caràcter personal:

- L'adreça electrònica: hi ha opinions diferents sobre això, ja que, d'una banda, autors com Aparicio es plantegen si l'adreça electrònica es pot considerar una dada de caràcter personal en aquells supòsits en els quals sigui formada pel nom del titular, i recorden que és necessari tornar a la idea inicial segons la qual, perquè hi hagi dada personal, fa falta una vinculació entre la informació i un subjecte concret: es necessiten dos components que se sotmetin a tractament. Per tant, l'adreça electrònica no s'hauria de considerar dada de caràcter personal mentre no aparegui associada a la persona que la utilitza.
  Tanmateix, l'AEPD va establir en un dictamen de l'any 1999 que l'adreça electrònica és una dada de caràcter personal tant en aquells casos en els

Lectura recomanada

J. Aparicio Salom (2009). *Estudio sobre la Ley orgánica de protección de datos de carácter personal*. Cizur Menor: Aranzadi.

quals identifica una persona perquè n'inclou el nom i cognoms o les inicials i conté informació relativa a l'empresa en la qual treballa o al país de residència, com en aquells altres en els quals no sembla mostrar dades relacionades amb la persona titular del compte (es refereix, per exemple, a una combinació alfanumèrica o denominació abstracta).

Fins i tot en aquest cas l'AEPD considera que sí que es tracta d'una dada de caràcter personal, ja que l'adreça electrònica apareixerà necessàriament referenciada a un domini concret, de tal manera que es pot procedir a la identificació del titular mitjançant la consulta del servidor en el qual es gestioni aquest domini, sense que això es pugui considerar que comporti un esforç desproporcionat de qui en fa la identificació.

Lectura recomanada

Informe de l'AEPD, "Dirección de correo electrónico" (1999).

- L'adreça IP: segons l'AEPD, "tot i que no sempre sigui possible per a tots els agents d'Internet identificar un usuari a partir de dades tractades a la Xarxa, des d'aquesta Agència de Protecció de Dades es parteix de la idea que la possibilitat d'identificar un usuari d'Internet existeix en molts casos i, per tant, les adreces IP, tant fixes com dinàmiques, amb independència del tipus d'accés, es consideren dades de caràcter personal i, en conseqüència, resulta aplicable la normativa sobre protecció de dades".

Lectura recomanada

Informe de l'AEPD núm. 327/2003, "Carácter de dato personal de la dirección IP".

- El número de telèfon, amb algun matís.

Lectures recomanades

Informes de l'AEPD núm. 285/2006, "Número de teléfono y carácter de dato personal", i núm. 575/2008, "Fichero con números de teléfono móvil".

- La matrícula d'un vehicle.

Lectura recomanada

Informe de l'AEPD núm. 425/2006, "Matrículas de vehículos y concepto de dato de carácter personal".

- Les mostres biològiques: són les mostres de matèria orgànica susceptibles de ser analitzades genèticament. Tanmateix, sense una anàlisi no s'aporta cap tipus d'informació, per la qual cosa la mostra biològica no constitueix per si mateixa una informació, no pot ser considerada una dada de caràcter personal, sinó que es tracta només d'una font d'informació. En canvi, el resultat de l'anàlisi serà constituït per un conjunt de dades que tindran caràcter personal quan es trobin associades a la identitat d'una persona determinada o determinable.

Lectura recomanada

J. Aparicio Salom (2009). *Estudio sobre la Ley orgánica de protección de datos de carácter personal*. Cizur Menor: Aranzadi.

- La veu i la imatge.

Lectures recomanades

Per a més informació, podeu consultar l'Informe de l'AEPD "Tratamiento de los registros de voz" (1999) i l'Informe de l'AEPD "Videovigilancia en el lugar de trabajo" (2001); Instrucció 1/2006, de 8 de novembre, de l'Agència Espanyola de Protecció de Dades, sobre el tractament de dades personals amb finalitats de vigilància mitjançant sistemes de càmeres o videocàmeres.

- El document nacional d'identitat.

Lectura recomanada

Podeu consultar l'Informe de l'AEPD núm. 476/2008, "Fichero con datos sobre personas jurídicas y DNI. Derecho de acceso, rectificación y oposición".

En definitiva, cada vegada es va ampliant més la categoria de dada de caràcter personal, i es passa d'un criteri d'identificabilitat a un altre de contactabilitat. Segons aquesta nova concepció, que entre d'altres propugna Poullet (2009), seria *dada de caràcter personal* aquella que permetés arribar a contactar amb una persona o bé seguir-ne el rastre, sense que en determinats casos calgués identificar-la amb noms i cognoms. En sentit semblant ja semblava que es pronunciava el Grup de l'art. 29, en el Dictamen 4/2007 sobre el concepte de *dades personals*, en què establia que el requisit de la identificabilitat no comporta necessàriament trobar el nom del subjecte en qüestió.

Lectura recomanada

Y. Poullet (2009, novembre). "Privacy: Conditions for its survival in our I.S". A: *31 Conferencia Internacional de autoridades de protección de datos y privacidad* (pàg. 8). Madrid. En línia:

<http://www.privacyconference2009.org/program/Presentaciones/index-ides-idweb.html>.

La LOPD resulta aplicable a qualsevol tipus de dada personal, amb independència de la seva rellevància, fins i tot si es tracta de dades que no incideixen en l'esfera d'intimitat de la persona. Aquesta definició tan àmplia del concepte de *dada de caràcter personal* no implica que totes les dades tinguin la mateixa importància i estiguin sotmeses al mateix règim jurídic, ja que algunes dades estan sotmeses a un règim de protecció més gran que d'altres (com els previstos en l'art. 7 LOPD) i d'altres estan subjectes a un tractament especial (per exemple, les dades relatives a la salut, segons l'art. 8 LOPD).

3.1.2. El terme *personal*

L'article 3.a LOPD estableix que es considera *dada de caràcter personal* qualsevol informació relativa a persones físiques identificades o identificables. Així, doncs, és necessari que la informació es pugui vincular a una persona física determinada i que aquesta vinculació es pugui dur a terme per mètodes que

no siguin complexos. La complexitat del mètode es pot valorar amb paràmetres subjectius (en funció de la capacitat tècnica de qui tracta les dades) o amb paràmetres objectius (en funció de l'estat de la tecnologia). El RLOPD estableix que una persona no es considerarà identificable si aquesta identificació requereix terminis o activitats desproporcionats.

a) Les dades relatives a una persona concebuda i no nascuda

El règim general de la protecció civil del *nasciturus* es troba regulat en els articles 29 i 30 CC. Per a determinar si les dades d'aquest *nasciturus* entren dins de l'àmbit d'aplicació de la LOPD, s'ha d'acudir a l'expressió "tots els efectes que li siguin favorables" de l'article 29 CC, és a dir, si aquest "efecte favorable" comprèn, també, la titularitat de drets fonamentals.

> "El naixement determina la personalitat; però la persona concebuda es té per nascuda per a tots els efectes que li siguin favorables, sempre que neixi amb les condicions que expressa l'article següent".
>
> (Article 29 CC)

Hi ha interpretacions tant en sentit afirmatiu com en sentit negatiu. Tanmateix, fins i tot en els supòsits en els quals es consideri que no es pot predicar l'existència de dades personals respecte al concebut, les dades que existeixin no queden desprotegides.

Lectura recomanada

Vegeu les dues interpretacions possibles sobre els drets del *nasciturus* a **P. Grimalt Servera** (1999). *La responsabilidad civil en el tratamiento automatizado de datos personales* (pàg. 49-51). Granada: Comares.

La protecció es pot atorgar en considerar que es tracta de dades que afecten la mare, per la qual cosa es tractaria de dades d'una persona física. Una altra possibilitat és considerar-les com a dades d'un grup familiar (algunes de les informacions de la persona concebuda poden afectar el grup familiar a què pertany o pertanyerà, com, per exemple, les dades genètiques), i amb aquesta configuració les dades també quedarien tutelades, en la mesura que es tractaria de dades personals.

b) Les dades relatives a un mort

Quant a les dades de les persones mortes, únicament podrien ser considerades com a dades personals, a efectes de la LOPD, les que es poguessin considerar dades característiques d'un grup familiar determinat –dades que, per tant, poden afectar la intimitat familiar– o bé les que directament o indirectament afectessin terceres persones.

Lectura recomanada

Així es pronuncia Grimalt respecte a la LORTAD. Aquest criteri també és aplicable al marc normatiu actual. Grimalt també indica que un tractament que lesionés la memòria de les persones mortes no deixaria d'estar tutelat per la Llei orgànica 1/1982.

P. Grimalt Servera (1999). *La responsabilidad civil en el tratamiento automatizado de datos personales* (pàg. 53 i 54). Granada: Comares.

Cal tenir en compte la previsió de l'article 2.4 RLOPD, que estableix que "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 adreçar als responsables dels fitxers o tractaments que continguin dades d'aquesta persona amb la finalitat de notificar l'òbit, aportar-ne prou

acreditació, i sol·licitar, quan escaigués, la cancel·lació de les dades". Per tant, únicament s'està atribuint una de les facultats del dret a la protecció de dades –la relativa a la cancel·lació– als familiars del mort.

Lectura recomanada

Sobre les dades de les persones mortes, vegeu:

R. Martínez Martínez (2008). "Principis i aspectes clau del nou Reglament". A: J. Marí; M. Vilasau (coord.). *El Reglament de protecció de dades: aspectes clau* (pàg. 28-30). Barcelona: UOC.

c) Les dades relatives a les persones jurídiques

Per a determinar si les persones jurídiques poden ser titulars dels drets reconeguts en la LOPD, abans cal plantejar-se si les persones jurídiques poden ser titulars de drets fonamentals. La CE no dóna una resposta expressa a la qüestió i ha estat la jurisprudència constitucional la que ha reconegut a les persones jurídiques aquells drets fonamentals que, tenint en compte el seu objecte i finalitat, poden ser-los d'utilitat (inviolabilitat del domicili, tutela judicial efectiva, secret de les comunicacions i llibertat d'expressió i informació).

Lectura recomanada

Per a tots aquests casos, vegeu:

L. Díez-Picazo Jiménez (2005). *Sistema de derechos fundamentales* (pàg. 133-136). Madrid: Civitas. L'autor critica la solució donada per alguna STC que reconeix el dret a l'honor a una persona jurídica, ja que considera que l'honor és una característica profundament humana.

Respecte al dret a la intimitat, Díez-Picazo assenyala que les persones jurídiques no es poden considerar titulars d'aquest dret, ja que no tenen vida personal ni familiar, i considera molt dubtós que el dret a la protecció de dades correspongui a les persones jurídiques, a més que l'article 3 LOPD només fa referència a les persones físiques.

L'article 18.4 CE es refereix als ciutadans quant a subjectes protegits. Els articles 1.1 i 2.a de la Directiva 95/46/ fan referència a la protecció de les persones físiques, i la mateixa referència es fa en els articles 1, 3.a i 3.e LOPD. En aquest sentit, el considerant 24 de la Directiva 95/46/CE determina que:

Lectura recomanada

L. Díez-Picazo Giménez. *Sistema de derechos* (pàg. 288-312). Madrid: Civitas.

> "Les legislacions relatives a la protecció de les persones jurídiques respecte del tractament de les dades que les concerneixin no són objecte d'aquesta Directiva."

D'altra banda, l'article 2.2 RLOPD estableix expressament que el Reglament en qüestió no és aplicable als tractaments de dades referides a persones jurídiques. La conclusió és que pel que fa a aquestes últimes no es pot predicar l'existència de dades de caràcter personal i, per tant, queden excloses de l'àmbit d'aplicació de la LOPD.

d) Les dades relatives a l'empresari individual

Un altre interrogant que sorgeix és què succeeix respecte a l'empresari individual. Les dades d'un subjecte que exerceixi una activitat empresarial o professional estan subjectes a la LOPD? La qüestió es planteja perquè de vegades aquestes dades poden fer referència tant a l'esfera professional com a l'esfera privada.

Abans de l'entrada en vigor del RLOPD, l'AEPD havia declarat que, en cas de dubte sobre el tipus de dada, calia presumir que la dada afectava la vida privada, de manera que, tret que hi hagués una prova en contra, calia entendre que

les dades relatives a un empresari individual n'afectaven la vida privada i no l'empresarial. La prova del caràcter de les dades s'havia de fer cas per cas, analitzant també la finalitat del tractament a fi de determinar la protecció aplicable.

Amb l'entrada en vigor del RLOPD es van aclarir una mica els interrogants, ja que, d'una banda, l'article 2.2 RLOPD no s'aplica "als tractaments de dades referides a persones jurídiques, ni als fitxers que es limitin a incorporar les dades de les persones físiques que els prestin els seus serveis, que consisteixin en el nom i cognoms, les funcions o llocs exercits, i també l'adreça postal o electrònica, el telèfon i el número de fax professionals".

D'altra banda, l'article 2.3 RLOPD també exclou del règim d'aplicació de la protecció de dades, les dades dels empresaris individuals quan es refereixin a la seva qualitat de comerciants, industrials o naviliers. Per tant, a la resta de dades de caràcter personal diferents de les esmentades en aquest precepte, sí els resulten aplicables la LOPD i el RLOPD. Així mateix, els professionals que actuen per compte d'altri o que no són organitzats en forma d'empresa, no són inclosos en l'article.

Lectura recomanada

Resposta 6, pàg. 8, primera sessió de l'AEPD (2008).

També cal tenir en compte els aclariments fets per l'AEPD en la primera sessió oberta (2008) sobre els problemes, la interpretació i l'aplicació del RLOPD. Perquè operin les excepcions dels apartats 2 i 3 de l'article 2 del RLOPD, és necessari que es compleixin els requisits següents:

Lectura recomanada

Resposta 3, pàg. 5, primera sessió de l'AEPD (2008). Informe de l'AEPD núm. 42/2008, "Novedades Reglamento: empresarios individuales".

- Les dades s'han de limitar a les enumerades en l'article 2.2 RLOPD per a les persones de contacte.

- Les dades dels comerciants (art. 2.3 RLOPD) han d'estar vinculades exclusivament amb l'activitat empresarial, és a dir, referir-se a la condició de comerciant, industrial o navilier. Aquesta excepció no opera quan les dades que s'hagin de tractar es refereixin a l'esfera personal del comerciant o quan no es refereixin a l'activitat empresarial, com succeeix, per exemple, quan l'objecte de tractament sigui l'empresari que ha constituït l'empresa i no l'activitat empresarial en si mateixa.

- El tractament ha de tenir com a destinatari l'empresa, mai la persona física.

3.1.3. Fitxer o tractament de dades

La LOPD, a diferència de la LORTAD, resulta aplicable tant als tractaments automatitzats com als no automatitzats.

D'altra banda, la Directiva 95/46, en l'article 3.1, estableix que les seves disposicions són aplicables:

> "[...] al tractament totalment o parcialment automatitzat de dades personals, i també al tractament no automatitzat de dades personals contingudes o destinades a ser incloses en un fitxer."

Respecte als tractaments no automatitzats de dades, encara que els resultava aplicable la Directiva, estaven sotmesos a un règim transitori (ex article 32.2 de la Directiva 95/46/CE i disposició addicional [DA] 1.2 LOPD) segons el qual s'establia un termini de dotze anys per a adequar-se a la LOPD. Transcorregut aquest termini, que va finalitzar el 24 d'octubre de 2007, la LOPD resulta plenament aplicable als tractaments no automatitzats, si bé el RLOPD estableix un règim transitori respecte a l'aplicació de les disposicions relatives a les mesures de seguretat dels fitxers, automatitzats o no, que ja existien en el moment de la seva entrada en vigor (disposició transitòria [DT] 2a. RLOPD).

Lectures recomanades

L'article 2.1 LORTAD feia referència al fet que la Llei era aplicable a les dades de caràcter personal que figuressin en fitxers *automatitzats*. L'article 2.1 LOPD disposa, simplement, que la norma és aplicable a les dades de caràcter personal registrades en un suport físic. L'article 5.1n RLOPD defineix què cal entendre per *tractaments no automatitzats*.

S'ha d'efectuar una precisió respecte a l'aplicació de la LOPD a fitxers i tractaments de dades, ja que no tenen per què coincidir, és a dir, les operacions que implica un tractament de dades no tenen perquè coincidir amb les del fitxer, ja que tant l'AEPD com els tribunals han sancionat d'una manera diferenciada responsables de fitxers i responsables de tractaments.

Exemples de sancions

AEPD, Procediment sancionador núm. PS/00588/2008, i AEPD, Procediment sancionador núm. PS/00460/2007. Sentència del Tribunal Suprem, Sala Tercera (Sala Contenciosa Administrativa), de 5 de juny de 2004.

3.1.4. Tractaments regulats per la LOPD

Una vegada determinat si ens trobem davant d'una dada de caràcter personal i que hi ha un tractament o fitxer organitzat, caldrà veure si, a raó del tractament, la LOPD resulta aplicable. En aquest sentit, la LOPD en determina l'àmbit d'aplicació de tres maneres:

a) Regulant els fitxers que es regeixen per la LOPD (art. 2.1 LOPD, segon paràgraf).

b) Determinant els fitxers que en queden exclosos (art. 2.2 LOPD). Aquests són els fitxers mantinguts per persones físiques en l'exercici de les seves activitats personals o domèstiques, els quals estan sotmesos a la normativa sobre protecció de matèries classificades i els establerts per a la investigació del terrorisme i de la delinqüència organitzada. En aquest últim cas, el responsable del fitxer ha de comunicar prèviament l'existència del fitxer, les seves característiques i la seva finalitat a l'AEPD. Quant als fitxers denominats *d'ús domèstic*, s'ha de tenir molt present el cas Lindqvist, que va fer una aplicació més aviat restrictiva d'aquesta excepció. La STJCE de 3 de novembre 2003 va establir, entre altres aspectes, que el fet de tenir una pàgina web i penjar-hi informació relativa als qui impartien catequesi en una parròquia no es podia considerar inclòs dins de l'excepció de l'àmbit domèstic. Segons el TJCE, l'excepció de l'article 3.2.II de la Directiva 95/46 s'ha d'interpretar en el sentit que preveu únicament les activitats que s'inscriuen en el marc de la vida privada o familiar dels particulars i no considera com a tals la difusió de dades per Internet, de manera que resultin accessibles a un grup indeterminat de persones (par. 47).

Lectura recomanada

E. Suñé Llinás (2002). "Introducción y protección de datos personales". A: *Tratado de derecho informático* (vol. I, 2a. ed., pàg. 148). Madrid: Universidad Complutense, Facultad de Derecho, Servicio de Publicaciones.

Aquest autor considera que l'exclusió dels fitxers de caràcter domèstic sense cap altre requisit comporta una aplicació massa incondicionada de la Directiva, ja que és possible que es tracti de fitxers que tinguin, per exemple, un contingut racista.

c) Establint la submissió d'uns fitxers a disposicions específiques i a les disposicions expressament previstes en la mateixa LOPD (art. 2.3 LOPD).

3.2. Obligacions prèvies al tractament de les dades: creació, modificació i supressió de fitxers

Abans d'iniciar el tractament de qualsevol dada de caràcter personal, cal seguir uns passos determinats, i complir unes obligacions determinades, entre les quals destaca la creació dels fitxers corresponents.

Lectures recomanades

L'article 26.1 LOPD, que prescriu que tota persona que procedeixi a la creació de fitxers de dades de caràcter personal ho ha de notificar prèviament a l'AEPD, i l'article 52.2 RLOPD, segons el qual la disposició o l'acord que estableixi la creació, la modificació o la supressió d'un fitxer de titularitat pública, s'haurà de dictar i publicar amb caràcter previ a la creació, la modificació o la supressió del fitxer.

La LOPD fa referència a aquest aspecte en el títol IV, que porta la rúbrica "Disposicions sectorials", i dedica el capítol I als fitxers de titularitat pública i el capítol II, als fitxers de titularitat privada. La LOPD estableix un tractament diferenciat entre els fitxers de titularitat pública i els fitxers de titularitat privada, respecte a la creació de fitxers i al règim sancionador aplicable, i atorga als primers un tractament certament privilegiat.

3.2.1. Creació, modificació i supressió de fitxers de titularitat pública

Els fitxers de titularitat pública comprenen els de les administracions públiques o d'altres ens, organismes o corporacions de dret públic. Tot i així, hi ha casos en els quals és dubtós determinar si es tracta d'un fitxer de titularitat pública o de titularitat privada, aspecte que s'aborda en els subapartats *l* i *m* de l'article 5.2 RLOPD. Aquest últim precepte proporciona una definició més aviat restrictiva de *fitxer de titularitat pública*, la qual cosa comporta una reducció del nombre de fitxers subjectes a la competència de les autoritats de control autonòmiques.

Lectura recomanada

Sobre els conceptes de *fitxer públic* i *fitxer privat*, vegeu:

S. Farré Tous (2008). "Novetats del RLOPD per a les administracions públiques". A: J. Marí; M. Vilasau (coord.). *El Reglament de protecció de dades* (pàg. 103 i següents). Barcelona: UOC.

Normativa a Catalunya sobre la protecció de dades de caràcter personal en els fitxers de titularitat pública

També incideixen en les definicions de *fitxer de titularitat pública* i *fitxer de titularitat privada* altres normes amb rang superior al RLOPD, com, per exemple, en el cas de Catalunya, l'Estatut d'autonomia de Catalunya (EAC), que preveu en l'article 156 que correspon a la Generalitat de Catalunya 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 la inscripció i el control d'una sèrie de fitxers o tractaments que s'hi enumeren, enumeració que és més àmplia que la que es deriva del RLOPD. Per tant, i a raó del seu rang normatiu, per determinar quan ens trobem davant d'un fitxer de titularitat pública o privada, en el cas de Catalunya ens haurem d'atenir al que disposa l'EAC.

La creació, modificació i supressió de fitxers de titularitat pública només es pot dur a terme per mitjà d'una disposició general publicada en el *Butlletí Oficial de l'Estat* (BOE) o en el diari oficial corresponent amb caràcter previ a la creació, modificació o supressió del fitxer (art. 20.1 LOPD i 52 RLOPD). Aquesta disposició o acord de creació, modificació o supressió haurà d'indicar el que preveuen els articles 20.2 LOPD i 54 RLOPD. En aquest últim supòsit, la disposició que es dicti en què s'acordi la supressió dels fitxers haurà d'establir la destinació que es donarà a les dades o, si escau, les previsions que s'han d'adoptar per a la seva destrucció (art. 20.3 LOPD i 54.3 RLOPD).

També cal tenir en compte que

"tot fitxer de dades de caràcter personal de titularitat pública ha de ser notificat a l'AEPD per l'òrgan competent de l'Administració responsable del fitxer per a la seva inscripció en el Registre General de Protecció de Dades, en el termini de trenta dies a comptar de la data de publicació de la norma o de l'acord de creació en el diari oficial corresponent."

(Art. 55.1 RLOPD)

"Quan l'obligació de notificar afecti fitxers subjectes a la competència d'una autoritat de control autonòmica que hagi creat el seu propi registre de fitxers, la notificació s'ha de fer a l'autoritat autonòmica competent, que trasllada la inscripció al Registre General de Protecció de Dades."

(Art. 55.3 RLOPD)

3.2.2. Creació, modificació i supressió de fitxers de titularitat privada

Segons l'article 25 LOPD, es poden crear fitxers de titularitat privada que continguin dades de caràcter personal quan d'una manera acumulativa es compleixin els requisits següents:

- Quan resulti necessari per a la consecució de l'activitat o l'objecte legítims de la persona, empresa o entitat titular.

- Quan es respectin les garanties que estableix la LOPD per a la protecció de les persones.

L'article 26.1 LOPD estableix que la creació de fitxers de dades de caràcter personal s'ha de notificar prèviament a l'AEPD. La notificació ha d'identificar el fitxer i el seu responsable, la finalitat i els usos previstos, el sistema de trac-

tament emprat en la seva organització (automatitzat, manual o parcialment automatitzat), el col·lectiu de persones afectat, la procedència de les dades i el procediment d'obtenció, les categories de dades, el servei o unitat davant del qual es pot exercir el dret d'accés, el nivell de mesures de seguretat i, si escau, la identificació de l'encarregat del tractament on es trobi ubicat el fitxer i els destinataris de cessions i transferències internacionals de dades.

3.2.3. Notificació de fitxers al Registre General de Protecció de Dades

Una vegada creat el fitxer mitjançant una disposició de caràcter general en el cas de les administracions públiques, o comunicada la seva existència a l'autoritat de control competent, el Registre General de Protecció de Dades procedeix a la inscripció del fitxer si la notificació s'ajusta als requisits exigibles; és a dir, la inscripció és reglada si es compleixen els requisits legals. En cas contrari, el Registre pot demanar que es completi la informació que falta o bé que es procedeixi a l'esmena corresponent. La inscripció s'entén concedida no solament per resolució expressa, sinó també per silenci positiu d'un mes.

Quan l'obligació de notificar afecti fitxers subjectes a la competència de l'autoritat de control d'una comunitat autònoma que hagi creat el seu propi registre de fitxers, la notificació l'ha de fer l'autoritat autonòmica competent, que trasllada la inscripció al Registre General de Protecció de Dades de l'AEPD.

3.3. Legitimació per al tractament de les dades de caràcter personal

Un dels principis bàsics de la LOPD és el del consentiment de la persona interessada per al tractament de les seves dades de caràcter personal, que actua com a mecanisme de legitimació d'aquest tractament. Ara bé, hi ha altres formes de legitimació –admeses per la Llei– per a tractar les dades i que no passen pel consentiment de la persona afectada:

- Quan la llei així ho estableix expressament.
- Quan les dades consten en fonts accessibles al públic.
- Quan les dades s'han obtingut a partir d'una altra persona (o empresa) diferent de la interessada, és a dir, quan hi ha hagut una cessió de dades.
- Quan es tracta de satisfer un interès legítim del responsable del tractament.
- Quan es tracta de complir un deure imposat per una norma.

Per a procedir al tractament de dades de caràcter personal, prèviament cal facilitar una informació determinada a la persona afectada. L'article 5 LOPD estableix el deure d'informació i determina quina informació cal proporcionar

en el moment de recollir les dades. Els apartats 1, 2 i 3 d'aquest article fan referència a la regla general i els apartats 4 i 5, als casos en els quals es produeixi un tractament de dades sense que, com a punt de partida, hagi entrat en joc el consentiment de la persona interessada o afectada.

L'apartat 4 de l'article 5 LOPD estableix com a regla general la necessitat d'informar la persona afectada d'una manera expressa, precisa i inequívoca, dins dels tres mesos següents al moment del registre de les dades, del contingut del tractament, de la procedència de les dades i del previst en les lletres *a*, *d* i *e* de l'apartat 1 d'aquest article 5 LOPD. Resulta criticable que la LOPD permeti diferir fins a tres mesos aquesta comunicació a la persona interessada, tenint en compte que l'article 11 de la Directiva estableix aquesta obligació "a comptar del moment del registre de les dades". D'altra banda, l'article 5.5 LOPD estableix una sèrie d'excepcions a aquest deure d'informar la persona interessada.

No s'ha d'oblidar que en aquests supòsits, en la mesura que les dades s'han obtingut sense consentiment previ de la persona interessada, aquesta té la facultat d'oposar-se'n al tractament (art. 6.4 i 30.4 LOPD i 34-36 RLOPD).

3.3.1. El consentiment de la persona interessada

A l'hora d'obtenir dades directament de la mateixa persona interessada, aquesta haurà de ser informada d'una manera expressa, precisa i inequívoca, entre altres aspectes, de l'existència del tractament i de la finalitat de la recollida de les dades (art. 5.1.a LOPD).

Lectura recomanada

Sobre això, podeu consultar l'article 18 RLOPD, que tracta sobre l'acreditació del compliment del deure d'informació.

> Al seu torn, l'article 4.2 LOPD preveu que "les dades de caràcter personal objecte de tractament no es poden usar per a finalitats incompatibles amb aquelles per a les quals les dades han estat recollides. No es considera incompatible el tractament posterior d'aquestes dades amb finalitats històriques, estadístiques o científiques".

Per tant, el consentiment es dóna per a un tractament que té una finalitat concreta: no és un consentiment abstracte o genèric, sinó per a un tractament concret i que no es pot considerar atorgat per a una finalitat diferent, però sí perquè no sigui incompatible. Aquesta exigència de consentir un tractament concret, per a unes finalitats determinades, explícites i legítimes, és un dels principis fonamentals del tractament de dades, l'anomenat *principi de finalitat* o *de qualitat de les dades*, recollit en l'article 4 LOPD, que comporta que les dades de caràcter personal siguin adequades, pertinents i no excessives respecte a la finalitat per a la qual s'obtenen i siguin exactes i actualitzades. Es tracta, al seu torn, d'assegurar la veracitat i l'exactitud de les dades obtingudes i tractades. D'altra banda, la Llei també estableix quan no es considera una finalitat incompatible el tractament amb finalitat estadística, històrica o científica (art. 4.2 LOPD i 9 RLOPD).

a) Regla general: consentiment inequívoc de la persona afectada

L'article 6.1 LOPD recull la regla general per al tractament de les dades de caràcter personal, segons la qual és necessari el consentiment inequívoc de la persona afectada, tret que la llei disposi una altra cosa. L'article 10.1 RLOPD estableix que "les dades de caràcter personal únicament poden ser objecte de tractament o cessió si la persona interessada n'hagués donat prèviament el consentiment" i l'article 12.1 RLOPD preveu que "el responsable del tractament haurà d'obtenir el consentiment de la persona interessada per al tractament de les seves dades de caràcter personal, excepte en aquells supòsits en els quals el mateix no sigui exigible d'acord amb el que disposen les lleis". Correspon a aquest responsable la prova de l'existència del consentiment de la persona afectada (art. 12.3 RLOPD).

L'article 3.h LOPD determina què s'entén per *consentiment de la persona interessada*: "tota manifestació de voluntat, lliure, inequívoca, específica i informada, mitjançant la qual la persona interessada consenti el tractament de dades personals que li concerneixen". La referència al "consentiment inequívoc" ha estat interpretada per algun autor per contraposició al consentiment exprés i per escrit que exigeix la LOPD en l'article 7.2 i ha considerat que consentiment inequívoc no s'hauria d'identificar amb consentiment exprés.

Lectura recomanada

A. Téllez Aguilera (2001). *Nuevas tecnologías y protección de datos: Estudio sistemático de la Ley orgánica 15/1999* (pàg. 150). Madrid: Edisofer.

b) El consentiment tàcit

Per *declaració tàcita de voluntat* s'entén aquella en la qual es fa un determinat acte o comportament dels quals es permet deduir que la voluntat existeix.

Lectura recomanada

L. M. Díez-Picazo y Ponce de León (2007). *Fundamentos del derecho civil patrimonial*. Vol. I: *Introducción: Teoría del contrato* (6a. ed., pàg. 148-149). Madrid: Civitas.

Alguns autors admeten que l'article 6.1 LOPD comprèn la declaració tàcita de voluntat sempre que la persona afectada –entenent com a tal un subjecte mitjà– tingui una consciència clara del que comporta aquesta declaració. Les actuacions en massa de les empreses fan necessari l'atorgament del consentiment tàcit, ja que és molt complex sol·licitar el consentiment d'una manera individual i expressa de cada client potencial.

Lectures recomanades

J. Aparicio Salom (2009). *Estudio sobre la Ley orgánica de protección de datos de carácter personal*. Cizur Menor: Aranzadi.

A. Téllez Aguilera (2001). *Nuevas tecnologías y protección de datos: Estudio sistemático de la ley orgánica 15/1999* (pàg. 150). Madrid: Edisofer.

Informe de l'AEPD, núm. 93/2008, "Formas de obtener el consentimiento mediante web: consentimientos tácitos".

c) El valor del silenci

Com s'ha de valorar el silenci? El silenci es pot considerar com una declaració en tots aquells casos en els quals la bona fe imposa un deure positiu de manifestar una repulsa. Alguns autors admeten que en el tractament de dades el silenci té valor positiu, i així sembla que ho va admetre l'AEPD en la Recomanació al sector del comerç electrònic de 24 de juliol de 2001.

L'article 14 RLOPD aborda aquesta qüestió i regula com es pot obtenir el consentiment i el valor que cal atorgar al silenci en aquells supòsits en els quals no és necessari el consentiment exprés per al tractament de les dades de caràcter personal. Aquest precepte permet al responsable del tractament adreçar-se a la persona afectada, complint els deures d'informació previstos en els articles 5 LOPD i 12 RLOPD, i concedir-li un termini de trenta dies perquè manifesti la seva negativa al tractament, i advertir-li que, en cas de no manifestar-se sobre

això, s'entén que consent el tractament (art. 14.2 RLOPD). Per tant, s'estableix una regla de silenci positiu: si no es diu res en un temps determinat, s'entén que es consent.

Perquè entri en joc aquesta regla és necessari que el responsable del tractament pugui conèixer si la comunicació ha estat objecte de devolució per qualsevol causa; en aquest cas, no pot procedir al tractament de les dades de caràcter personal referides a la persona interessada (art. 14.3 RLOPD).

A més, caldrà facilitar a la persona interessada un mitjà senzill i gratuït perquè pugui manifestar la seva negativa al tractament de les dades de caràcter personal, com, per exemple, la tramesa prefranquejada al responsable del tractament o la trucada a un número de telèfon gratuït (art. 14.4 RLOPD).

Una vegada el responsable hagi utilitzat aquest procediment a fi d'obtenir el consentiment de la persona interessada, no és possible tornar a sol·licitar el consentiment per als mateixos tractaments i per a les mateixes finalitats en el termini d'un any a comptar de la data de la sol·licitud anterior (art. 14.5 RLOPD).

Aquest mecanisme d'obtenció del consentiment ha generat força polèmica. El sector del màrqueting i de les empreses de comunicació considera que és confús, ja que cal deixar constància de totes les trameses efectuades i que no s'ha rebut una negativa. D'altra banda, també caldrà poder acreditar la data concreta en la qual s'han efectuat les trameses, a fi de poder-ho tornar a fer una vegada transcorregut un any, si així es vol. A més, aquestes mesures poden resultar costoses econòmicament i organitzativament per a les petites i mitjanes empreses, ja que la majoria no té telèfons habilitats gratuïts ni disposen de sobres prefranquejats.

Aquest article s'ha criticat des d'altres àmbits, ja que la solució adoptada és contrària a la jurisprudència del Tribunal Suprem relativa al valor del silenci respecte als particulars, els subjectes que no són comerciants, i ha posat en relleu que un reglament no pot anar en contra d'aquesta jurisprudència.

Cal remarcar que, encara que s'hi hagi donat el consentiment, aquest és revocable quan hi hagi una causa justificada i no se li atribueixin efectes retroactius (art. 6.3 LODP i 17 RLOPD).

d) Excepcions a la regla general del consentiment

Lectura recomanada

L. M. Díez-Picazo y Ponce de León (2007). *Fundamentos del derecho civil patrimonial* (pàg. 150-151). Madrid: Civitas.

Lecturas recomanadas

J. Aparicio Salom (2009). *Estudio sobre la Ley orgánica de protección de datos de carácter personal*. Cizur Menor: Aranzadi.

P. A. de Miguel Asensio (2002). *Derecho privado de Internet* (3a. ed., pàg. 551-552). Madrid: Civitas.

Malgrat la regla general que s'ha exposat, en determinats casos no farà falta el consentiment de la persona interessada:

- 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.

- Quan les dades es refereixin a les parts d'un contracte o un precontracte d'una relació negocial, laboral o administrativa, i siguin necessàries per al manteniment o compliment de la relació.

- Quan el tractament tingui per finalitat protegir un interès vital de la persona interessada en els termes de l'article 7.6 LOPD.

- Quan 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 de la tercera persona a qui es comuniquin les dades, sempre que no es vulnerin els drets i les llibertats fonamentals de la persona interessada (art. 3.j, 28 i 30 LOPD).

En els casos en els quals es puguin tractar les dades de caràcter personal sense que sigui necessari el consentiment de la persona afectada i sempre que una llei no disposi el contrari, la persona afectada es pot oposar al tractament de les dades quan tingui motius fonamentats i legítims relatius a una situació personal concreta. En aquest cas, el responsable del fitxer ha d'excloure del tractament les dades relatives a la persona afectada (art. 6.4 i 30.4 LOPD, i 34 i 35 RLOPD).

e) Consentiment reforçat: dades especialment protegides

El legislador ha considerat que determinades dades de caràcter personal han de tenir un nivell de protecció més gran. La manera d'aconseguir-ho consisteix a atorgar més protecció a determinades dades que es consideren especialment sensibles, mitjançant l'establiment d'uns requisits més estrictes per a obtenir el consentiment de la persona afectada. Per a això ha establert diferents nivells de protecció, en funció del tipus de dades de què es tracti:

- Nivell més intens de protecció: les dades només poden ser objecte de tractament amb el consentiment exprés i per escrit de la persona afectada (art. 7.2 LOPD).

Partint de l'article 16.2 CE, que prescriu que ningú no pot ser obligat a declarar sobre la seva ideologia, religió o creences, l'article 7.1 LOPD estableix que

> "quan amb relació a aquestes dades (ideologia, religió o creences) es procedeixi a demanar el consentiment a què es refereix l'apartat següent, s'ha d'advertir la persona interessada sobre el seu dret a no donar-lo."

El nivell màxim de protecció s'estableix respecte a les dades que revelin ideologia, afiliació sindical, religió o creences. Per a tractar aquestes dades fa falta el consentiment exprés i per escrit de la persona afectada. Tanmateix, s'exceptuen d'aquest règim reforçat els fitxers mantinguts per partits polítics, sindicats, esglésies, confessions o comunitats religioses i associacions, fundacions i altres entitats sense ànim de lucre, la finalitat dels quals sigui política, filosòfica, religiosa o sindical, respecte a les dades relatives als seus associats o membres. Ara bé, per a la cessió d'aquestes dades fa falta sempre el consentiment previ de la persona afectada.

- Nivell menys intens de protecció: les dades només poden ser objecte de tractament amb el consentiment exprés de la persona afectada o quan així ho disposi una llei, per raons d'interès general (art. 7.3 LOPD).

Alguns autors no consideren justificada la diferència de requisits que s'estableix per a obtenir el consentiment entre les dades incloses en l'article 7.2 LOPD i les de l'article 7.3 LOPD, ja que sembla indicar una certa jerarquia entre les diferents dades examinades, i defensen que les dades recollides en els dos preceptes tenen el mateix valor. Per tant, els requisits han de ser els mateixos i en els supòsits previstos en l'article 7.3 LOPD també faria falta el consentiment exprés i per escrit a l'hora d'obtenir les dades.

Lectura recomanada

A. Téllez Aguilera (2001). *Nuevas tecnologías, intimidad y protección de datos. Estudio sistemático de la ley orgánica 15/1999* (pàg. 130). Madrid: Edisofer.

Sembla raonable aquest plantejament, sobretot tenint en compte que algunes dades, com, per exemple, les referents a la vida sexual, estan bastant lligades a la ideologia. Malgrat això, en aquests casos legalment no es requereix el consentiment per escrit.

Malgrat el que preveuen en els apartats anteriors, les dades especialment protegides també poden ser objecte de tractament sense consentiment de la persona interessada quan siguin necessàries per a:

- La prevenció o el diagnòstic mèdics.

- La prestació d'assistència sanitària o de tractaments mèdics o la gestió de serveis sanitaris.

- Salvaguardar l'interès vital de la persona afectada o d'una altra persona, en cas que estigui físicament o jurídicament impossibilitada per a donar el seu consentiment.

Finalment, cal tenir en compte que la recollida i el tractament de les dades enumerades en els apartats 2 i 3 de l'article 7 LOPD per part de les forces i dels cossos de seguretat, estan sotmesos a un règim específic (art. 22.3 LOPD).

3.3.2. Dades subjectes a una normativa específica

Respecte a les dades relatives a la salut, l'article 8 LOPD remet a una normativa específica, de manera que "les institucions i els centres sanitaris públics o privats i els professionals corresponents poden procedir al tractament de les dades de caràcter personal relatives a la salut de les persones que hi acudeixin o que hi hagin de ser tractades, d'acord amb el que disposa la legislació estatal o autonòmica sobre sanitat".

Altres dades sensibles i que tenen una regulació específica són les relatives a la comissió d'infraccions penals o administratives. Aquestes dades només poden ser incloses en fitxers de les administracions públiques competents en els supòsits previstos en les respectives normes reguladores (art. 7.5 LOPD).

3.3.3. El consentiment per al tractament de les dades dels menors

El tractament de les dades de caràcter personal dels menors no és un tema que s'abordi d'una manera específica en la LOPD.

Abans de l'entrada en vigor del RLOPD, calia recórrer al marc normatiu general per a donar una resposta als interrogants que es plantejaven.

La situació ha canviat amb el nou RLOPD, ja que regula expressament aquesta qüestió en l'article 13 RLOPD.

Segons aquest precepte, es pot procedir al tractament de les dades de caràcter personal dels majors de catorze anys amb el seu consentiment, excepte en aquells casos en els quals la llei exigeixi per al seu atorgament l'assistència dels titulars de la pàtria potestat o tutela. En el cas dels menors de catorze anys, es requereix el consentiment dels pares o tutors. En cap cas no es poden recollir dades del menor que permetin obtenir informació sobre els restants membres del grup familiar o sobre les seves característiques, com per exemple dades relatives a l'activitat professional dels progenitors, informació econòmica, dades sociològiques o d'altres, sense el consentiment dels titulars d'aquestes dades. No obstant això, es poden recollir les dades d'identitat i adreça del pare, la mare o el tutor amb l'única finalitat d'obtenir l'autorització prevista en l'apartat anterior.

Quan el tractament es refereixi a dades dels menors d'edat, la informació que se'ls adreci s'haurà d'expressar en un llenguatge que sigui fàcilment comprensible per als menors.

Lectura recomanada

I. Gómez-Juárez Sidera (2006). "Reflexiones sobre el derecho a la protección de datos de los menores de edad y la necesidad de su regulación específica en la legislación española". *Revista Aranzadi de Derecho y Nuevas Tecnologías* (núm. 2).

Lectura recomanada

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. Llei orgànica 1/1996, de 15 de gener, de protecció jurídica del menor, LOPD i Codi civil o legislació civil de les respectives comunitats autònomes.

El responsable del fitxer o tractament haurà d'articular els procediments que garanteixin que s'ha comprovat d'una manera efectiva l'edat del menor i l'autenticitat del consentiment atorgat, si escau, pels pares, tutors o representants legals. Per tant, allò que el responsable del tractament ha d'acreditar és que ha establert uns mecanismes adequats de control de l'edat, si bé és possible que aquests controls puguin ser burlats. L'article 13 RLOPD també ha estat un precepte una mica polèmic, en la mesura que hi ha qui considera que en cap cas no correspon a un reglament regular aquest aspecte, i més tenint en compte que es contradiu en alguns casos amb normes de rang superior.

Lectura recomanada

P. Grimalt Servera (2008). "El consentimiento y el tratamiento con fines publicitarios y prospección comercial". A: J. Marí; M. Vilasau (coord.). *El Reglament de protecció de dades* (pàg. 71-78). Barcelona: UOC.

Si bé considerem que són encertades algunes crítiques que es formulen en l'article 13 RLOPD, també és cert que aquest precepte tracta de proporcionar protecció a les dades dels menors que naveguen per la Xarxa. Constantment es produeix un intercanvi de dades sobre els menors i entre els menors, especialment a les xarxes socials, de les quals són uns dels usuaris principals. Per tant, encara que possiblement la solució proporcionada no sigui des d'un punt de vista dogmàtic la més correcta, sí que tracta de proporcionar solucions concretes.

3.3.4. Dades procedents de fonts accessibles al públic

La LORTAD ja va establir com a excepció a la necessitat del consentiment de la persona afectada el fet que les dades constessin en fonts accessibles al públic. L'article 3.j LOPD entén per *fonts accessibles al públic* el següent:

> "[...] aquells fitxers la consulta dels quals pot ser feta per qualsevol persona, no impedida per una norma limitadora o sense més exigència que, si escau, l'abonament d'una contraprestació".

Si bé la necessitat de disposar del consentiment de la persona afectada s'exceptua en el cas de les fonts accessibles al públic, només constitueix excepció l'obtenció del consentiment, i no el dret que té la persona afectada a ser informada sobre el tractament de les seves dades i l'exercici dels seus drets. Per aquest motiu, l'article 5.5 LOPD estableix que, quan les dades procedeixin de fonts accessibles al públic i es destinin a l'activitat de publicitat o prospecció comercial, en cada comunicació que es dirigeixi a la persona interessada se l'ha d'informar de l'origen de les dades i de la identitat del responsable del tractament i també dels drets que l'assisteixen.

A més, l'article 6.2 LOPD estableix uns matisos importants. Partint de la premissa que es tracti d'una dada procedent de fonts accessibles al públic, fa falta que:

- El tractament de les dades sigui necessari per a la satisfacció d'un interès legítim del responsable del fitxer o de la tercera persona a qui es comuniquin les dades.

- No es vulnerin els drets i les llibertats fonamentals de la persona afectada.

Les fonts accessibles al públic constitueixen una llista de *numerus clausus*, ja que només tenen la consideració de fonts d'accés públic:

a) El cens promocional

Segons disposa l'article 31 LOPD, els subjectes que es dediquin d'una manera habitual o esporàdica a la recopilació d'adreces, venda a distància, repartiment de publicitat o prospecció comercial, poden obtenir de l'Institut Nacional d'Estadística o dels òrgans equivalents de les comunitats autònomes una còpia del cens promocional format pel nom, els cognoms i el domicili que consten al cens electoral. Aquesta llista té la vigència d'un any, transcorregut el qual deixarà de ser considerada com a font accessible al públic.

La LOPD permet donar als censos electorals un ús comercial. Alguns autors critiquen que el cens promocional tingui una validesa anual, ja que aquest fet pot comportar que únicament les grans empreses de publicitat directa, venda a distància, màrqueting, etcètera, es puguin permetre disposar d'aquesta eina. Aquesta limitació, assenyalen, pot ocasionar que proliferi el mercat negre de dades, que és una de les coses que es pretén evitar amb la LOPD.

Aspectes com el procediment de formació del cens promocional, el dret a oposar-se a aparèixer en el cens, la posada a disposició dels sol·licitants o el control de les llistes difoses, es van deixar a un desplegament reglamentari futur (art. 31 i DT 2a. LOPD). No obstant això, el RLOPD no tracta cap d'aquests aspectes, ja que l'article 7.1.a RLOPD es limita a enumerar el cens promocional com una font accessible al públic, sense entrar a regular res més. En la pràctica, el cens promocional és una font que no existeix.

b) Repertoris telefònics o guies de comunicacions electròniques en els termes previstos per la seva normativa específica

Es tracta d'una norma oberta que es remet als límits que fixi la normativa que reguli aquests repertoris. La legislació actual sobre això és la Llei 32/2003, de 3 de novembre, general de telecomunicacions (LGT).

L'article 22.b LGT estableix que, entre els serveis que integren el servei universal, s'haurà de garantir

> "[...] que es posi a disposició dels abonats al servei telefònic disponible al públic una guia general de números d'abonats, impresa o electrònica, o ambdues, i s'actualitzi, com a mínim, una vegada l'any. Així mateix, que es posi a disposició de tots els usuaris finals d'aquest servei, inclosos els usuaris de telèfons públics de pagament, almenys un servei d'informació general sobre números d'abonats. Tots els abonats al servei telefònic disponible al públic tenen dret a figurar en aquesta guia general, sense perjudici, si escau, del respecte a les normes que regulin la protecció de les dades personals i el dret a la intimitat."

A més, l'article 38.6 LGT preveu, entre els drets dels consumidors i usuaris, que en l'elaboració i comercialització de les guies d'abonats als serveis de comunicacions electròniques i la prestació dels serveis d'informació sobre ells cal garantir als abonats el dret a la protecció de les seves dades personals, inclòs el de no figurar en aquestes guies.

La LGT va ser desplegada pel Reial decret 424/2005, de 15 d'abril, norma que també preveu l'obligació de posar a disposició dels abonats una guia general de números d'abonats i un servei d'informació general o consulta telefònica sobre números d'abonats (art. 27.2, RD 424/2005).

Lectura recomanada

Reial Decret 424/2005, de 15 d'abril, pel qual s'aprova el Reglament sobre les condicions per a la prestació de serveis de comunicacions electròniques, el servei universal i la protecció dels usuaris, *Butlletí Oficial de l'Estat* (BOE), núm. 102, 29 d'abril de 2005, pàg. 14545 i següents.

c) Llistes de professionals

Perquè tinguin la consideració de fonts accessibles al públic, aquestes llistes han de contenir únicament les dades relatives al nom, títol, professió, activitat, grau acadèmic, adreça i indicació de la pertinença al grup. Per a qualsevol dada afegida fa falta el consentiment de la persona interessada, que pot ser revocat en qualsevol moment.

El RLOPD ha fet una petita puntualització referida a l'adreça professional, ja que estableix que aquesta "pot incloure les dades del domicili postal complet, número telefònic, número de fax i adreça electrònica". A més, preveu que "en el cas de col·legis professionals, es poden indicar com a dades de pertinença al grup els de número de col·legiat, data d'incorporació i situació d'exercici professional".

D'altra banda, la persona interessada pot sol·licitar que es faci constar que les seves dades no es poden utilitzar per a finalitats de prospecció comercial o de publicitat i a més també té el dret a exigir gratuïtament l'exclusió de la totalitat de les seves dades personals que constin al cens promocional.

d) Els diaris i butlletins oficials i els mitjans de comunicació

L'article 3.j LOPD fa referència al fet que els diaris i butlletins oficials tenen el caràcter de fonts accessibles al públic, sense fer cap tipus de delimitació. La informació que es publica és molt diversa i pot incloure, per exemple, dades relatives a infraccions o nomenaments determinats. Per aquest motiu, s'ha indicat que seria convenient una certa cautela a l'hora de publicar dades de caràcter personal en els butlletins i diaris oficials. Sobre això és molt interessant la Recomanació 1/2008, de l'Agència Catalana de Protecció de Dades, sobre la difusió d'informació que contingui dades de caràcter personal per Internet i, concretament el capítol III, dedicat a la publicació en diaris oficials i butlletins oficials electrònics.

Respecte als mitjans de comunicació, cal remarcar que l'AEPD considera que Internet no és un mitjà de comunicació, per la qual cosa no té el caràcter de font accessible al públic.

En la primera sessió oberta organitzada per l'AEPD (2008), aquesta va posar de manifest que

> "[...] es poden considerar incloses en fonts accessibles al públic les dades que hagin estat objecte de difusió per la premsa, ràdio i televisions (convencional o digital). Les revistes purament científiques no s'haurien de considerar font accessible al públic als efectes de l'aplicació de la LOPD. Internet no és, als efectes de protecció de dades, un «mitjà de comunicació social», sinó un «canal de comunicació», per la qual cosa no és una font accessible al públic".

Enllaç recomanat

Primera sessió oberta de l'AEPD (2008), pàg. 10, de les preguntes més freqüents (PMF):

<https://www.agpd.es/portalweb/jornadas/1_sesion_abierta/common/faqs_bloque_1.pdf>.

3.3.5. L'existència d'un interès legítim i el compliment d'una obligació legal

El RLOPD estableix que, malgrat la regla general segons la qual les dades de caràcter personal no es poden tractar sense el consentiment de la persona interessada, en aquells casos en els quals ho autoritzi una norma amb rang de llei o una norma de dret comunitari sí que es poden tractar en els supòsits següents (art. 10.2.a RLOPD):

- Quan el tractament o la cessió tinguin per objecte la satisfacció d'un interès legítim del responsable del tractament o del cessionari emparat per les normes i sempre que no prevalguin l'interès o els drets i les llibertats fonamentals dels interessats (ex article 1 LOPD).

- Quan el tractament o la cessió de les dades siguin necessaris perquè el responsable del tractament compleixi un deure que li imposi una norma.

Aquest precepte trasllada a l'ordenació espanyola l'article 7.f de la Directiva 95/46, que encara no havia estat incorporat al nostre ordenament. Tanmateix, és dubtós que s'hagi adaptat correctament la norma comunitària. L'article 7.f de la Directiva 95/46 permet el tractament de les dades sense el consentiment de l'interessat en els supòsits que sigui necessari per a la satisfacció de l'interès legítim del responsable del tractament. Tanmateix, la regla continguda en l'article 10.2.a estableix, com hem vist, un pressupòsit: "Quan ho autoritzi una norma amb rang de llei o una norma de dret comunitari". Això constitueix un prerequisit que no apareix en la Directiva i que restringeix l'àmbit d'aplicació que s'ha tractat d'introduir en el nostre ordenament.

Així mateix, el supòsit en el qual la Llei permeti el tractament ja es preveu expressament en l'article 6.1 LOPD *in fine*, per la qual cosa el primer paràgraf de l'article 10.2.a seria redundant.

3.4. L'obtenció de les dades a partir d'un subjecte diferent de la persona interessada

Una altra manera d'obtenir o accedir a les dades de caràcter personal és perquè un subjecte diferent de la persona interessada les ha comunicat. Dins d'aquest supòsit, es plantegen dues situacions: les que es consideren cessió o comunicació de dades i les que no es consideren cessió de dades.

3.4.1. Accessos que es consideren cessió de dades

La cessió de dades de fitxers de titularitat privada es troba regulada en els articles 11 i 27 LOPD. Perquè aquesta cessió sigui legítima s'han de complir d'una manera cumulativa dos requisits:

- La necessitat de la comunicació per al compliment de les finalitats directament relacionades amb les funcions legítimes del cedent i el cessionari.

- El consentiment previ de la persona interessada (art. 10.1 i 12.2 RLOPD).

D'altra banda, segons preveu l'article 11.3 LOPD, el consentiment per a la comunicació de dades és nul quan la informació que es proporcioni a la persona interessada no li permeti conèixer la finalitat a què es destinaran les dades la comunicació de les quals s'autoritza, o bé el tipus d'activitat de la persona a la qual es pretenen comunicar. En el mateix sentit, es pronuncia l'article 12.2 RLOPD, que ha emfatitzat encara més la necessitat que quedi clara la finalitat a què es destinaran les dades objecte de la cessió.

El responsable del fitxer, quan efectuï la primera cessió de dades, haurà d'informar les persones afectades sobre (art. 27.1 LOPD):

- la finalitat del fitxer,
- la naturalesa de les dades que han estat cedides,
- el nom i l'adreça del cessionari.

Tot i així, en determinats casos (art. 27.2 LOPD) no existeix aquesta obligació d'informació.

L'article 19 RLOPD preveu que, en els supòsits en els quals es produeixi una modificació del responsable del fitxer com a conseqüència d'una operació de fusió, escissió, cessió global d'actius i passius o altres operacions de reestructuració societària de naturalesa anàloga prevista per la legislació mercantil, no es produeix cap cessió de dades, sens perjudici del que estableix l'article 5 LOPD.

Un supòsit concret que té una regulació específica és el de la cessió de dades relatives a la solvència patrimonial i el crèdit (art. 29 LOPD). Així mateix, un altre supòsit especial de cessió de dades és el previst en la DA 6a. LOPD, relatiu als fitxers de les entitats asseguradores, ja que les cessions de dades a aquests fitxers no requereixen el consentiment previ de la persona interessada.

Finalment, cal recordar que el dret d'informació que garanteix la LOPD preveu, entre altres aspectes, el dret a sol·licitar i obtenir informació gratuïta sobre les comunicacions de dades dutes a terme o que es pretenguin dur a terme (art. 15.1 LOPD).

Malgrat el principi del consentiment, la llei també preveu una sèrie d'excepcions a la necessitat del consentiment en la cessió de dades (art. 11.2 LOPD i 10.4 RLOPD):

- Quan la cessió sigui autoritzada per una llei.

- Quan es tracti de dades recollides de fonts accessibles al públic. En aquest cas, cal tenir en compte l'article 21.3 LOPD, sobre la comunicació de dades obtingudes de fonts accessibles al públic per part de les administracions públiques i amb destinació a fitxers de titularitat privada, ja que fa falta o bé el consentiment de la persona afectada o que la llei expressament ho prevegi.

- Quan el tractament respongui a l'acceptació lliure i legítima d'una relació jurídica el desenvolupament, compliment i control de la qual impliquin necessàriament la connexió d'aquest tractament amb fitxers de terceres persones.

- Quan la comunicació que calgui efectuar tingui com a destinataris el defensor del poble, el Ministeri Fiscal, els jutges i els tribunals o el Tribunal de Comptes.

- Quan la cessió es produeixi entre administracions públiques i tingui per objecte el tractament posterior de les dades amb finalitats històriques, estadístiques o científiques (vegeu l'art. 21 LOPD).

- Quan la cessió de dades relatives a la salut sigui necessària per a solucionar una urgència o per a elaborar determinats estudis.

El consentiment per a la comunicació de dades de caràcter personal també és revocable (art. 6.3 LOPD i 17 RLOPD).

Quant a les obligacions del cessionari –aquell a qui es comuniquen les dades de caràcter personal–, pel sol fet de la comunicació, ha de dur a terme les disposicions de la LOPD.

Respecte a les dades especialment protegides, l'article 7.2 LOPD exigeix que el consentiment per a la cessió sigui previ, però no que sigui exprés i per escrit, com en el cas de l'obtenció de dades. Malgrat això, s'hauria d'aplicar el mateix règim proteccionista en ambdós casos. L'article 10.1 RLOPD també fa referència al fet que el consentiment per a la cessió ha de ser previ, tal com estableix expressament l'article 11.1 LOPD.

3.4.2. Comunicació de dades entre administracions públiques

La comunicació de dades entre administracions públiques es troba regulada en l'article 21 LOPD. Aquest precepte preveu que les dades de caràcter personal recollides per una administració pública per a l'exercici de les seves atribucions no es poden comunicar a altres administracions públiques que exerceixin competències diferents o que versin sobre matèries diferents. S'admet la cessió encara que no es compleixi aquesta excepció quan el tractament posterior es faci amb finalitats històriques, estadístiques o científiques.

Sentència del Tribunal Constitucional sobre l'article 21.1 LOPD

L'article 21.1 LOPD va ser declarat parcialment inconstitucional mitjançant la STC 292/2000, de 30 de novembre, que va declarar nul l'incís que permetia la comunicació de dades d'una administració a una altra quan la disposició de creació del fitxer o una disposició de rang superior així ho hagués previst.

3.4.3. Accessos que no es consideren cessió de dades: l'encàrrec de tractament

Segons l'article 12.1 LOPD no es considera comunicació de dades l'accés d'una tercera persona a les dades quan aquest accés sigui necessari per a la prestació d'un servei al responsable del tractament. L'article 20 RLOPD desplega aquest precepte i estableix una precisió interessant: es considera que hi ha una comunicació de dades quan l'accés tingui com a objectiu l'establiment d'un vincle nou entre qui accedeix a les dades i la persona afectada.

Quan una tercera persona hagi d'intervenir d'alguna manera en el tractament de les dades, segons la previsió de l'article 12.2 LOPD, s'haurà de formalitzar un contracte entre el responsable del tractament i la tercera persona. Aquest contracte haurà de constar per escrit o d'alguna altra manera que en permeti acreditar la formalització i el contingut. Haurà de recollir que l'encarregat del tractament únicament haurà de tractar les dades conforme a les instruccions del responsable del tractament, que no les ha d'aplicar ni utilitzar amb finalitats diferents de les previstes en el contracte, ni les ha de comunicar, ni tan sols per a la conservació, a altres persones.

S'estableixen, així mateix, les mesures de seguretat que l'encarregat del tractament està obligat a implementar.

En els casos en els quals es vulgui contractar la prestació d'un servei que comporti un tractament de dades de caràcter personal, caldrà vetllar perquè la persona contractada ofereixi garanties que complirà el que preveu el Reglament. Per tant, s'imposa un deure de cura al responsable del fitxer a l'hora d'escollir l'encarregat del tractament.

Una vegada complerta la prestació contractual, les dades de caràcter personal s'hauran de destruir o tornar al responsable del tractament. L'article 22 RLOPD introdueix uns matisos importants:

- Una vegada finalitzada la prestació contractual, les dades de caràcter personal s'hauran de destruir o tornar al responsable del tractament o a l'encarregat que el primer hagi designat (art. 22.1 RLOPD).

- No és procedent la destrucció de les dades quan hi hagi una previsió legal que així ho estableixi (art. 22.1 RLOPD).

- L'encarregat del tractament pot conservar les dades convenientment bloquejades durant el temps en què es puguin reclamar responsabilitats derivades de la seva relació amb el responsable del tractament (art. 22.2 RLOPD).

En el cas d'incompliment per part de l'encarregat del tractament, aquest es considera responsable del tractament i ha de respondre de les infraccions en què hagi incorregut personalment (art. 12.4 i 20.3 RLOPD). Tot i així, segons preveu l'article 20.3 RLOPD, l'encarregat del tractament no incorre en responsabilitat quan, després d'haver-ho indicat expressament i prèviament, el responsable, comuniqui les dades a una tercera persona designada pel responsable.

Una novetat important del RLOPD és la regulació de la possibilitat de subcontractació dels serveis per l'encarregat del tractament. D'entrada, l'article 21.1 RLOPD estableix que l'encarregat del tractament només pot subcontractar una tercera persona si ha obtingut autorització del responsable del tractament per a fer-ho. En aquest cas, la contractació s'ha d'efectuar sempre en nom i per compte del responsable del tractament. Ara bé, l'article 22.2 RLOPD també preveu que sigui possible la subcontractació sense necessitat d'autorització del responsable del tractament previ compliment dels requisits previstos en el mateix article 22.2 RLOPD.

3.5. Seguretat i confidencialitat en el tractament de les dades

Vegem a continuació els deures de seguretat i de confidencialitat exigits en el tractament de les dades de caràcter personal.

3.5.1. El deure de seguretat en el tractament de les dades de caràcter personal

La LOPD estableix en l'article 9 un deure, a càrrec del responsable del fitxer i de l'encarregat del tractament, dirigit a garantir la seguretat de les dades i evitar-ne l'alteració, la pèrdua, el tractament o l'accés no autoritzat, i que comporta la necessitat d'adoptar les mesures necessàries per a aconseguir-ho.

Aquest deure de seguretat o de diligència s'estableix amb relació a uns paràmetres concrets: l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estiguin exposades. Si la tecnologia determina, en la mesura del que sigui possible, la naturalesa de les dades que cal protegir ofereix el criteri del que és raonable.

Els requisits de seguretat comporten que no es registraran dades de caràcter personal en els fitxers que no compleixin les condicions que s'estableixin per via reglamentària. Respecte a les dades especialment sensibles, l'article 9.3 LOPD remet al Reglament per establir els requisits i les condicions que han de reunir els fitxers i les persones que intervinguin en el tractament.

A l'hora de regular la seguretat que requereix un tractament de dades, la clau rau en les "mesures d'índole tècnica i organitzatives necessàries que garanteixin la seguretat de les dades personals". El RLOPD es converteix en l'instrument normatiu bàsic en matèria de seguretat de fitxers o tractaments, automatitzats o no, i representa i comporta, entre altres obligacions, la necessitat de plasmar en un document de seguretat la política de seguretat definida en l'organització.

La finalitat de les mesures de seguretat és garantir la confidencialitat, la integritat i la disponibilitat de les dades.

El Reglament estableix tres nivells de seguretat: bàsic, mitjà i alt, segons la naturalesa de la informació tractada –el tipus de dades–, amb relació a la necessitat més o menys gran de garantir la confidencialitat i la integritat de la informació. L'article 81 RLOPD estableix quan correspon aplicar un determinat nivell de seguretat. El nivell bàsic s'ha d'aplicar a tots els fitxers o tractaments de dades i el nivell superior inclou totes les mesures dels nivells inferiors. Aquests nivells tenen la condició de mínim exigible; per tant, no hi ha cap obstacle per a optar per un nivell de seguretat superior.

L'element clau de la política de seguretat d'un sistema d'informació ha de quedar reflectit en el document de seguretat, que registra d'una manera actualitzada tota la informació rellevant sobre com s'efectua el tractament de les dades i el contingut del qual es regula en l'article 88 RLOPD.

Respecte a les mesures de seguretat concretes que integren cada nivell, el RLOPD distingeix entre els tractaments automatitzats (art. 89 a 104 RLOPD) i els tractaments no automatitzats (art. 105 a 114 RLOPD). A fi de determinar quines mesures de seguretat són exigibles, també cal tenir en compte les disposicions transitòries. La DT 2a. RLOPD preveu els terminis d'implantació de les mesures de seguretat relatives als tractaments que ja existien quan va entrar en vigor aquest Reglament (que distingia novament entre tractaments automatitzats i tractaments no automatitzats). Els fitxers creats posteriorment a l'entrada en vigor del RLOPD hauran d'implantar la totalitat de les mesures

de seguretat des del moment de la seva creació. Així mateix, quant a la regulació de la seguretat pel que fa a l'Administració pública, s'ha de tenir en compte el Reial decret 3/2010, de 8 de gener, pel qual es regula l'esquema nacional de seguretat en l'àmbit de l'Administració electrònica. Aquest Reial decret desenvolupa l'article 42.2 de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, i busca establir els principis i requisits d'una política de seguretat en la utilització de mitjans electrònics que permeti una protecció adequada de la informació.

3.5.2. El deure de secret

El responsable del fitxer i les persones que intervinguin en qualsevol fase del tractament de les dades de caràcter personal estan obligats al secret professional respecte a les dades que tracten. Aquestes obligacions han de subsistir fins i tot després de finalitzada la relació amb el titular o responsable del fitxer.

3.6. La regulació de determinats fitxers

Per a alguns tipus de fitxers s'estableixen regles especials.

3.6.1. Els fitxers de les forces i dels cossos de seguretat

La recollida i el tractament de dades amb finalitat policial sense el consentiment de les persones afectades es troben regulats en l'article 22.2 LOPD, i la recollida de les dades considerades especialment sensibles es regula en l'article 22.3 LOPD.

Lectura recomanada

Sobre fitxers policials, vegeu:
R. Martínez Martínez (2001). *Tecnologías de la información, policía y Constitución.* València: Tirant lo Blanch.

Respecte als fitxers de les forces i dels cossos de seguretat, s'estableixen una sèrie d'excepcions als drets d'accés, rectificació i cancel·lació (art. 23 LOPD). Aquest precepte preveu la possibilitat que es denegui l'accés a les dades contingudes als fitxers en qüestió, la seva rectificació o cancel·lació, per motius relacionats amb la defensa de l'Estat, la seguretat pública, la protecció dels drets i de les llibertats de terceres persones o les necessitats d'investigacions en curs.

L'article 24 LOPD també preveu alguns supòsits de limitació dels drets de les persones afectades; concretament, la del dret d'informació a la persona afectada previst en l'article 5.1 de la LOPD quan aquesta informació afecti la defensa nacional, la seguretat pública o la persecució d'infraccions penals.

STC sobre els apartats 1 i 2 de l'article 24 LOPD

La STC 292/2000, de 30 de novembre, va declarar parcialment inconstitucional l'apartat 1 de l'article 24 LOPD i l'apartat 2, totalment inconstitucional.

3.6.2. Els fitxers de solvència patrimonial i crèdit

L'article 29 LOPD regula els fitxers que contenen dades relatives a la solvència patrimonial i el crèdit. Aquest tema va centrar l'atenció de la doctrina i de l'AEPD, que va dictar sobre això la Instrucció 1/1995, d'1 de març, relativa a la prestació de serveis d'informació sobre solvència patrimonial i crèdit. La cessió d'informació relativa a la solvència patrimonial comporta una excepció

al règim general del consentiment de la persona afectada motivada per una raó d'interès públic: la protecció del tràfic econòmic. Aquest precepte ha estat desplegat pels articles 37-44 RLOPD.

L'article 29 LOPD estableix dos supòsits diferents:

- El primer supòsit és aquell en el qual la informació sobre solvència patrimonial i crèdit objecte de tractament s'ha obtingut d'un registre o de fonts accessibles al públic establerts per a això, o bé ha estat facilitada per la mateixa persona interessada o amb el seu consentiment.

- El segon supòsit és aquell en el qual la informació relativa al compliment o incompliment d'obligacions dineràries ha estat facilitada pel creditor. En aquest cas, s'aplica una excepció al principi del consentiment i, concretament, a la cessió de dades sense el consentiment de la persona afectada o interessada. Es refereix als casos en els quals hi ha una obligació dinerària determinada que no s'ha complert (per exemple, un rebut retornat). El creditor, basant-se en l'excepció que estableix la LOPD, pot comunicar aquesta dada (l'impagament) a una altra persona que fa un tractament sobre insolvència patrimonial.

Aquesta comunicació de dades, que en funció de l'article 11.1 LOPD requeriria el consentiment previ de la persona afectada (deutora), es pot fer, segons l'article 29.2 LOPD, sense aquest consentiment i fins i tot, en el moment d'efectuar-se, sense el seu coneixement, ja que el cessionari té trenta dies per a comunicar la persona afectada que ha estat inclosa en un fitxer de solvència patrimonial (els anomenats *fitxers de morosos*).

Cal posar en relleu que es produeixen dues comunicacions de dades: una primera comunicació entre el creditor i el fitxer de solvència patrimonial i crèdit, i una altra comunicació del responsable d'aquest últim fitxer comú cap a les persones que el consultin, això són, les terceres persones que sol·liciten informació sobre possibles deutors.

El RLOPD ha endurit els requisits per al tractament d'aquestes dades, fruit dels abusos que s'havien produït en el passat amb relació a aquests fitxers. En conseqüència, ha fixat unes condicions molt estrictes perquè es puguin incloure i tractar dades en els fitxers comuns de solvència patrimonial, la qual cosa exigeix que es presentin els requisits següents (art. 38 i 39 RLOPD):

1) Existència prèvia d'un deute cert, vençut i exigible que hagi estat impagat i respecte al qual no s'hagi interposat una reclamació.

2) Transcurs de temps inferior als sis anys des de la data en la qual s'havia de pagar el deute o des del venciment de l'obligació o el termini concret.

3) Requeriment previ de pagament a qui correspongui el compliment de l'obligació.

4) Prohibició d'incloure en fitxers d'aquesta naturalesa dades personals respecte a les quals hi hagi un principi de prova que d'una manera indiciària contradigui algun dels requisits anteriors.

5) Informació al deutor prèvia a la inclusió en aquests fitxers.

6) Necessitat que sigui el mateix creditor, o bé qui actuï per compte i interès seu, qui faciliti la informació destinada als fitxers de solvència patrimonial i crèdit.

7) Notificació a la persona interessada (deutora), en el termini de trenta dies a comptar de la inclusió en el registre, d'una referència a les dades relatives a la seva persona que s'hagin inclòs, i també del dret a sol·licitar informació.

8) Comunicació del responsable del tractament, quan la persona interessada ho sol·liciti, de les dades i les avaluacions i apreciacions que hagin estat comunicades a terceres persones.

Respecte a l'exercici dels drets d'accés, rectificació, cancel·lació i oposició (ARCO), l'article 44 RLOPD distingeix en funció de davant de qui s'exerceixen aquests drets: davant la persona que ha facilitat les dades (el cedent), davant el responsable del fitxer comú, davant el cessionari de la informació o bé davant qualsevol altra entitat que participi en el sistema.

3.6.3. Els fitxers de publicitat i prospecció comercial

El tractament de fitxers amb finalitat de publicitat i prospecció comercial es regula en els articles 30 LOPD i 45-51 RLOPD. Representa un intent de conciliar el respecte a la intimitat amb el que es diu *màrqueting relacional*. Les campanyes de bustiada sovint ofereixen regals a canvi de dades de l'usuari i tenen com a finalitat obtenir perfils determinats. Una vegada les dades es troben higienitzades i prou relacionades entre elles, es poden traçar perfils dels usuaris, segmentar la base de clients, adaptar les ofertes als seus gustos i, en definitiva, incrementar els beneficis de l'empresa.

En primer lloc, cal tenir en compte en quins supòsits es poden tractar les dades de caràcter personal per a les finalitats de màrqueting, publicitat, venda a distància, prospecció comercial o altres activitats anàlogues:

a) Quan les dades de caràcter personal figurin en fonts accessibles al públic i no consti l'oposició o negativa de la persona interessada a rebre comunicacions comercials. Tot i així, subsisteix el deure d'informació que estableixen els articles 30.2 LOPD i 45.2 RLOPD quan es facin comunicacions comercials i les dades s'hagin obtingut de fonts accessibles al públic.

b) Quan les dades hagin estat facilitades per la mateixa persona interessada o hagin estat obtingudes amb el seu consentiment.

En les campanyes publicitàries sovint succeeix que una empresa encarrega una campanya determinada a una altra empresa i qui fa efectivament la selecció de destinataris i la tramesa corresponent és aquesta última. L'article 46 RLOPD intenta delimitar la responsabilitat entre aquests dos subjectes que poden participar en la campanya publicitària, per determinar qui es considerarà responsable del tractament. El caràcter de responsable s'ha de determinar en funció de qui ha decidit els paràmetres identificatius dels destinataris.

Una novetat important del RLOPD és que es regulen les anomenades *llistes Robinson*, és a dir, la possibilitat de crear fitxers comuns de caràcter general o sectorial l'objectiu dels quals és evitar la tramesa de comunicacions comercials a persones que han manifestat la seva negativa o bé la seva oposició a rebre publicitat. A aquests efectes, els fitxers esmentats poden tenir les mínimes dades de caràcter personal imprescindibles per a identificar la persona afectada (art. 49 RLOPD).

Els articles 50 i 51 RLOPD regulen l'exercici dels drets ARCO i fan especial referència als supòsits de campanyes de màrqueting en les quals intervenen diferents subjectes: l'un que encarrega una campanya i l'altre que en delimita els paràmetres.

En els tractaments de dades amb finalitat publicitària i de prospecció comercial cal posar en relació la regulació de protecció de dades amb la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (LSSI), ja que regula, entre altres aspectes, les comunicacions comercials per via electrònica (art. 19 a 22 LSSI).

En la seva redacció originària, la LSSI va optar per una solució restrictiva a l'hora de permetre les comunicacions als consumidors potencials (sistema d'*opt-in*, de tal manera que quedava prohibida la tramesa de comunicacions publicitàries o promocionals per correu electrònic o un altre mitjà de comunicació electrònica equivalent que prèviament no haguessin estat sol·licitades o expressament autoritzades pels destinataris). Aquesta regulació va ser modificada per la LGT, que va traslladar a l'ordenament espanyol la Directiva 2002/58, sobre privacitat i comunicacions electròniques.

La redacció actual de l'article 21.1 LSSI estableix que la tramesa de publicitat per correu electrònic o qualsevol altre mitjà de comunicació electrònica equivalent està condicionada al consentiment previ del destinatari, tal com estableix l'article 13.1 de la Directiva 2002/58. Però tot seguit l'article 21.2 LSSI recull l'excepció prevista en l'article 13.2 de la Directiva, de manera que es pot remetre publicitat en aquells casos en els quals hi hagi una relació contractual prèvia, si el remitent ha obtingut les dades d'una manera lícita i s'utilitzen per a enviar publicitat relativa a productes o serveis similars als contractats inicialment. Així mateix, cal oferir al destinatari la possibilitat d'oposar-se al tractament en el moment de la recollida de les dades i en qualsevol comunicació ulterior amb el destinatari. Aquest consentiment pot ser revocat en qualsevol moment (art. 22.1 LSSI).

Modificació de diversos articles LSSI

La disposició final primera de la LGT modifica els articles 21, 22, 38.3.b, 38.4.d i 43.1 LSSI a fi d'adaptar-los a aquesta Directiva.

En definitiva, per a les comunicacions publicitàries o promocionals per via electrònica, pot succeir que, malgrat disposar d'una sèrie de dades per a poder dur a terme una campanya de màrqueting, les comunicacions no es puguin fer si falta el consentiment de la persona interessada a qui s'enviïn aquest tipus de comunicacions.

Si es tracta de comunicacions no electròniques, no resulta aplicable la LSSI i la normativa de referència és la LOPD i la relativa a publicitat.

3.6.4. Els fitxers comuns de les entitats asseguradores

Un altre supòsit que té una regulació específica són els fitxers comuns de les entitats asseguradores que contenen dades de caràcter personal per a la liquidació de sinistres i la col·laboració estadisticoactuarial (DA 6a. LOPD). La cessió de dades a aquests fitxers no requereix el consentiment previ de la persona afectada, però sí la comunicació a aquesta persona de la possible cessió de les seves dades personals a aquests fitxers. En aquest cas, cal indicar qui és el responsable del fitxer, a fi que la persona afectada pugui exercir els drets d'accés, rectificació i cancel·lació previstos en la llei.

També es poden establir fitxers comuns la finalitat dels quals sigui prevenir el frau en l'assegurança, sense que sigui necessari el consentiment de la persona afectada. Únicament fa falta la comunicació a la persona afectada, en la primera introducció de les seves dades i per part del responsable del fitxer, de les formes d'exercici dels drets d'accés, rectificació i cancel·lació.

En tot cas, les dades relatives a la salut només poden ser objecte de tractament amb el consentiment exprés de la persona afectada.

Aquest tractament específic que es fa dels fitxers de les companyies d'assegurances és altament criticable. S'introdueix una excepció que no està prevista en la Directiva 95/46/CE i que obeeix a una activitat reeixida de *lobby*. Així, doncs, s'estableix l'excepció, per a un sector concret, d'un dels principis estructurals en matèria de protecció de dades: el del consentiment. I això és així malgrat que, una vegada feta l'excepció, s'estableixi el deure de comunicació a la persona interessada. A més, en el cas de cessió de dades, no solament es fa una excepció respecte del principi del consentiment, sinó que la comunicació es fa amb caràcter general sobre "la possible cessió de les seves dades personals a fitxers comuns"; és a dir, que no s'estableix una obligació de comunicar en el moment en què s'efectua la cessió. La solució de la llei és encara més perjudicial per a l'interessat, ja que, òbviament, no estarà inquirint d'una manera constant sobre si s'ha efectuat o no una cessió de les seves dades.

Lectura recomanada

E. Suñé Llinás (2000). "Introducción y protección de datos personales" (pàg. 171-172). A: *Tratado de derecho informático* (vol. I, 2a. ed.). Madrid: Universidad Complutense, Facultad de Derecho, Servicio de Publicaciones / Instituto de Español de Informática y Derecho.

3.6.5. Els fitxers de videovigilància

L'increment en els últims temps de la instal·lació de videocàmeres en llocs públics i privats és un fenomen que s'ha produït no solament a Espanya, sinó també a països europeus, als Estats Units, al Canadà, etcètera. Els estats, les empreses i la ciutadania busquen en la videovigilància la solució a l'augment de la sensació d'inseguretat i a la demanda social creixent de seguretat. A aquest increment s'afegeix el fet d'una tecnologia cada vegada més senzilla i a preus assequibles per a la ciutadania, amb la qual cosa la proliferació d'aquests sistemes en els àmbits privat, públic i empresarial va en augment.

Un sistema de videovigilància generalment comporta un tractament d'imatges i/o de veus de persones, que, segons els articles 3.a LOPD i 5.1.f RLOPD, tenen la consideració de dades personals, ja que la majoria d'instal·lacions d'aquesta naturalesa possibiliten la identificació de persones físiques, encara que no totes, ja que hi ha sistemes de videovigilància que controlen sistemes de producció, el trànsit, etcètera, i que no tracten dades personals.

Aquest tractament de dades té unes característiques peculiars que fan que en alguns aspectes no encaixi fàcilment amb els conceptes de la normativa de protecció de dades, perquè requereix alguna especificació o matisació derivada de la naturalesa del tractament de dades. Per això, les autoritats de control han dictat instruccions a fi de regular, dins de l'àmbit de les seves competències, els tractaments de dades fetes mitjançant sistemes de videovigilància.

Lectures recomanades

Instrucció 1/2006, de 8 de novembre, de l'Agència de Protecció de Dades, sobre el tractament de dades personals amb finalitats de vigilància a partir de sistemes de càmeres o videocàmeres (BOE, núm. 296, 12 de desembre de 2006); Instrucció 1/2007, de 16 de maig, de l'Agència de Protecció de Dades de la Comunitat de Madrid, sobre el tractament de dades personals a partir de sistemes de càmeres o videocàmeres en l'àmbit dels òrgans i administracions públiques de la Comunitat de Madrid (*Butlletí Oficial de la Comunitat de Madrid* [BOCM], núm. 169, 18 de juliol de 2007); Instrucció de l'Agència Catalana de Protecció de Dades, núm. 1/2009, de 10 de febrer, sobre el tractament de dades de

caràcter personal mitjançant càmeres amb finalitats de videovigilància (*Diari Oficial de la Generalitat de Catalunya* [DOGC], núm. 5322, 19 de febrer de 2009).

Les regulacions efectuades per les autoritats de control han establert una sèrie de requisits, més o menys comuns, per als fitxers de videovigilància:

a) Àmbit d'aplicació: sistemes de vigilància mitjançant càmeres que permeten l'enregistrament, la captació, la transmissió, la conservació, l'emmagatzemament d'imatges i la reproducció en temps real. S'exclou l'àmbit domèstic (videointèrfons, enregistraments familiars, enregistraments de viatges, etcètera).

Els sistemes de videovigilància emprats per les forces i pels cossos de seguretat es regeixen per la seva legislació específica, encara que la Instrucció 1/2009 de l'Agència Catalana de Protecció de Dades sí que els inclou d'una manera parcial dins del seu àmbit d'aplicació.

b) Legitimitat del tractament: s'haurà de recórrer al règim general que estableix l'article 6 LOPD. En alguns casos, es requereix el consentiment de la persona afectada –per exemple, en el cas de les càmeres instal·lades en guarderies perquè els pares puguin veure els fills–, mentre que, en d'altres, aquest tractament pot ser necessari per al desenvolupament d'una relació laboral o l'exercici de les funcions pròpies d'una administració pública.

Lectura recomanada

J. L. Goñi Sein (2007). *La videovigilancia empresarial y la protección de datos personales: Estudios de protección de datos*. Madrid: Thomson Civitas.

c) Creació i inscripció del fitxer, excepte en els supòsits en els quals únicament es produeixi una captació d'imatges en temps real; en aquest supòsit, no es genera cap fitxer.

Lectura recomanada

Informe de l'AEPD núm. 212/2007, "Grabación de imágenes en tiempo real".

d) Dret d'informació: s'ha d'informar sobre l'enregistrament o la captació d'imatges mitjançant cartells informatius.

e) Anàlisi de la proporcionalitat de la utilització de videocàmeres: si és possible utilitzar un altre mitjà menys invasiu de la intimitat de les persones, no s'hauria d'utilitzar el sistema de videovigilància.

f) Aplicació de les mesures de seguretat i de la resta d'obligacions establertes per la LOPD i el RLOPD.

g) Formalització del contracte d'encàrrec de tractament de l'article 12 LOPD en aquells casos en els quals el manteniment del sistema de videovigilància el dugui a terme una empresa de seguretat i el personal d'aquesta empresa pugui accedir a les imatges.

La Instrucció 1/2009 de l'Agència Catalana de Protecció de Dades preveu l'elaboració d'una memòria, prèvia a l'inici de la captació d'imatges, que ha de recollir els aspectes clau del tractament: justificació de la legitimitat, proporcionalitat i finalitat del tractament, definició de les característiques del sistema, ubicació de les càmeres, període de conservació de les imatges, etcètera. La

confecció d'aquesta memòria busca la reflexió del responsable del fitxer sobre la naturalesa del tractament que està instal·lant, les obligacions que comporta i si ell mateix pot resultar excessivament intrusiu en l'esfera de la intimitat de les persones.

3.7. Exercici dels drets d'accés, rectificació, cancel·lació i oposició (ARCO) per la persona afectada

El títol III de la LOPD es dedica als drets de les persones, que es concreten en els drets d'accés, rectificació, cancel·lació i oposició, i que, segons el Tribunal Constitucional, Sentència 292/2000, "constitueixen el feix de facultats que emana del dret fonamental a la protecció de dades i serveixen a la funció capital que exerceix aquest dret fonamental: garantir a la persona un poder de control sobre les seves dades personals, la qual cosa només és possible i efectiva imposant a terceres persones aquests deures de fer".

L'article 17 LOPD fa una remissió reglamentària a l'establiment d'un procediment per a exercir els drets ARCO, que actualment regula el RLOPD en els títols III i IX del capítol II.

Els drets AROC tenen caràcter personalíssim (art. 23 RLOPD) i es configuren com a independents, de tal manera que no es pot entendre que l'exercici d'algun d'ells sigui requisit per a exercir-ne un altre (art. 24 RLOPD). Respecte als fitxers de les forces i dels cossos de seguretat, l'article 23 LOPD estableix una sèrie d'excepcions a l'exercici dels drets ARCO. La persona afectada a qui es denegui totalment o parcialment l'exercici dels seus drets, ho pot posar en coneixement de l'AEPD o de l'organisme corresponent de la comunitat autònoma, segons escaigui, i les autoritats de control s'hauran d'assegurar de la procedència o improcedència de la denegació.

Quan es tracti de dades de caràcter personal registrades en fitxers de titularitat privada, únicament se'n denega l'accés quan la sol·licitud sigui formulada per una persona diferent de l'afectada i no s'acrediti la representació (art. 23.3 RLOPD).

3.7.1. Disposicions generals

El títol III RLOPD estableix d'entrada unes previsions de caràcter general aplicables a l'exercici de qualsevol dret, tant respecte als fitxers públics com respecte als fitxers privats.

L'article 23 RLOPD assenyala que els drets ARCO tenen caràcter personalíssim i els ha d'exercir la persona afectada. Tot i així, quan es trobi en situació d'incapacitat o minoria d'edat que li impossibiliti l'exercici personal d'aquests drets, els pot exercir mitjançant el seu representant legal i també a partir d'un representant voluntari, expressament designat.

S'haurà de concedir a la persona afectada un mitjà senzill i gratuït per a l'exercici dels drets ARCO, exercici que en cap cas no pot representar un ingrés addicional per al responsable del tractament (art. 24.2 i 3 RLOPD).

El responsable del fitxer o tractament haurà d'atendre la sol·licitud d'exercici dels drets per la persona afectada encara que no hagi utilitzat el procediment establert específicament pel primer, sempre que la persona interessada hagi utilitzat un mitjà que permeti acreditar la tramesa i la recepció de la sol·licitud i que aquesta tingui tots els elements que exigeix el RLOPD (art. 24.5 RLOPD).

Quant al procediment per a l'exercici dels drets, l'article 25 RLOPD estableix que caldrà dirigir una comunicació al responsable del fitxer en la qual constin la identificació de la persona interessada –i de la representació, quan n'hi hagi–, la petició en la qual es concreta la sol·licitud, l'adreça a efectes de notificació, la data, la signatura del sol·licitant i els documents acreditatius de la petició que es formula.

El responsable del tractament ha de contestar en qualsevol cas, amb independència que els seus fitxers continguin o no dades de caràcter personal relatives a la persona afectada, i correspon al responsable del tractament la prova del compliment del deure de resposta (art. 25.2 i 25.5 RLOPD, respectivament). En cas que la sol·licitud no compleixi els requisits exigits, el responsable del fitxer n'haurà de demanar l'esmena (art. 25.3 RLOPD).

Cal destacar que l'exercici dels drets ARCO es pot modular per raons de seguretat pública en els casos i amb l'abast previst en les lleis (art. 25.7 RLOPD). Així mateix, quan les lleis aplicables a determinats fitxers estableixin un procediment especial per a la rectificació o cancel·lació de les dades que contenen, s'haurà d'atenir a la normativa específica (art. 25.8 RLOPD).

Si les persones afectades exerceixen els seus drets davant de l'encarregat del tractament, aquest ha de traslladar la sol·licitud al responsable del tractament perquè la resolgui, excepte en els casos en què en la relació responsable-encarregat s'hagi previst que aquest últim ha d'atendre les sol·licituds d'exercici de drets per compte del responsable (art. 26 RLOPD).

Qualsevol d'aquests drets s'exerceix mitjançant una sol·licitud dirigida al responsable del fitxer i que aquest haurà de resoldre dins dels terminis previstos, tot i que no disposi de dades de la persona afectada.

El responsable del fitxer ha de resoldre sobre la sol·licitud d'accés en el termini màxim d'un mes a comptar de la seva recepció. Si resol aquesta sol·licitud en sentit positiu, el responsable del fitxer disposa de deu dies més per a fer-la efectiva. En canvi, en el cas dels drets de rectificació, cancel·lació i oposició, la resposta s'ha de comunicar a la persona afectada en el termini de deu dies a comptar de la recepció de la sol·licitud.

Transcorreguts els terminis previstos sense que d'una manera expressa es respongui a la sol·licitud de la persona interessada, aquesta pot interposar la reclamació prevista en l'article 18 LOPD davant de l'autoritat de control competent.

3.7.2. Dret d'accés a les dades

Cal distingir entre el dret de consulta i el dret d'accés al fitxer.

El dret de consulta és el dret a conèixer –sol·licitant la informació al Registre General de Protecció de Dades– l'existència d'un determinat tractament de dades de caràcter personal, les seves finalitats i la identitat del responsable del tractament. El Registre General és de consulta pública i gratuïta (art. 14 LOPD).

El dret d'accés és el dret de la persona afectada a obtenir d'una manera gratuïta informació sobre si les dades que fan referència a la seva persona estan essent objecte de tractament, la finalitat del tractament que, si escau, s'estigui duent a terme, i també la informació disponible sobre l'origen d'aquestes dades i de les comunicacions fetes o que es preveu dur a terme (art. 27.1 RLOPD).

En virtut del dret d'accés, la persona afectada pot obtenir del responsable del tractament informació relativa a dades concretes, a dades incloses en un fitxer determinat o a la totalitat de les dades relatives a la seva persona. No obstant això, quan raons d'especial complexitat ho justifiquin, el responsable del fitxer pot sol·licitar als afectats l'especificació dels fitxers respecte als quals volen exercir el dret d'accés i, a aquests efectes, el responsable els haurà de facilitar una relació de tots els fitxers (art. 27.2 LOPD).

Aquest dret d'accés és independent del que atorguen als afectats les lleis especials i, en particular, la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú (art. 27.3 RLOPD).

L'article 28 RLOPD especifica com es materialitza el dret d'accés i estableix que la persona afectada pot optar per rebre la informació per un o diversos sistemes de consulta del fitxer (visualització en pantalla, escrit, còpia o fotocòpia enviada per correu, telecòpia, correu electrònic o altres sistemes de comunicació electrònica). Al seu torn, preveu restriccions per als sistemes de consulta del fitxer en funció de la configuració o implantació material del fitxer i de la naturalesa del tractament, sempre que el que s'ofereixi a la persona afectada sigui gratuït i asseguri la comunicació escrita si així ho exigeix.

El responsable del fitxer ha de proporcionar la informació, independentment del suport en el qual es faciliti, d'una manera llegible i intel·ligible, sense utilitzar claus o codis que requereixin l'ús de dispositius mecànics específics.

Aquest dret d'accés únicament es pot exercir en intervals no inferiors a dotze mesos. Si s'exerceix una altra vegada abans de transcórrer aquest termini, el responsable del fitxer o del tractament pot denegar l'accés a les dades de caràcter personal. En cas que la persona interessada acrediti un interès legítim, pot tornar a tenir accés a les dades abans del transcurs dels dotze mesos indicats (art. 15.3 LOPD i 30.1 RLOPD).

Cal tenir en compte que l'accés es pot denegar en els casos en què legalment així estigui previst (art. 23 LOPD i 30.2 RLODP).

3.7.3. Dret de rectificació i cancel·lació

L'article 4 LOPD recull el principi de qualitat de les dades, una de les concrecions del qual és la cancel·lació i substitució d'ofici de les dades de caràcter personal que siguin inexactes o innecessàries. Al seu torn, l'article 16 LOPD regula el dret de rectificació i cancel·lació. Aquests dos preceptes són les dues cares de la mateixa moneda. Per tant, cal rectificar o cancel·lar les dades de caràcter personal el tractament de les quals no s'ajusti al que disposa la Llei i, en particular, quan les dades resultin inexactes, incompletes o innecessàries (art. 16.2 LOPD).

El dret de rectificació és el dret de la persona afectada que es modifiquin les dades que siguin inexactes o incompletes (art. 31.1 RLOPD).

La cancel·lació comporta el bloqueig de les dades i la seva conservació únicament per a l'Administració i els tribunals per tal de determinar les responsabilitats nascudes del tractament (art. 16.3 LOPD). Per tant, *cancel·lar* no és sinònim d'*esborrar*, ja que és possible bloquejar les dades.

En la sol·licitud de rectificació, la persona interessada haurà d'indicar a quines dades es refereix i la correcció que s'hi ha de fer, i haurà d'acompanyar la sol·licitud de la documentació justificativa de la rectificació. En la sol·licitud de cancel·lació, la persona interessada haurà d'indicar a quines dades es refereix, i haurà d'aportar a aquest efecte la documentació que en justifiqui la cancel·lació (art. 32.1 RLOPD).

Si les dades rectificades o cancel·lades haguessin estat cedides prèviament, el responsable del fitxer haurà de comunicar la rectificació o cancel·lació efectuada al cessionari, en el mateix termini, perquè aquest procedeixi també a rectificar o cancel·lar les dades (art. 16.4 LOPD i 32.3 RLOPD).

No obstant això, en determinats casos la cancel·lació no escau (art. 16.5 LOPD): quan les dades de caràcter personal hagin de ser conservades durant els terminis previstos en les disposicions aplicables o, si escau, en les relacions

contractuals entre la persona o entitat responsable del tractament i la persona interessada que van justificar el tractament de les dades, o quan així ho estableixi una llei (art. 33 RLOPD).

3.7.4. El dret d'oposició

El dret d'oposició és el dret de la persona afectada que no es dugui a terme el tractament de les seves dades de caràcter personal o se cessi. Aquest dret es troba regulat en els articles 34-36 RLOPD.

Lectura recomanada

Sobre el dret d'oposició, vegeu:

M. T. Casado Cadarso; À. Vila Muntal (2008). "¿Puede la Administración pública ocultar la identidad del denunciante?". *Datospersonales.org* [article en línia] (núm. 34). <http://www.datospersonales.org>.

Aquest dret es pot exercir en els supòsits següents:

a) Tal com preveu l'article 6.4 LOPD, quan no sigui necessari el consentiment de la persona afectada per al tractament de les dades de caràcter personal. En aquest cas, si la llei no estableix el contrari, la persona afectada es pot oposar al tractament si hi ha motius fundats i legítims, relatius a una situació personal concreta. En aquest cas, en la sol·licitud d'exercici del dret d'oposició hauran de constar els motius fundats i legítims que justifiquin l'exercici del dret (art. 35.1 RLOPD).

b) Com disposa l'article 30.4 LOPD, quan es tracti de fitxers que tinguin per finalitat la realització d'activitats de publicitat i prospecció comercial (art. 34.b i 51 RLOPD). En aquest cas no fa falta adduir cap motivació.

c) Quan el tractament tingui per finalitat l'adopció d'una decisió referida a la persona afectada i basada únicament en un tractament automatitzat de les seves dades de caràcter personal (art. 13 LOPD i 34.c RLOPD). Segons l'article 13.1 LOPD, les persones interessades tenen dret a no veure's sotmeses a una decisió amb efectes jurídics sobre elles o que els afecti d'una manera significativa, que es basi únicament en un tractament automatitzat de dades destinat a avaluar determinats aspectes de la seva personalitat, com el rendiment laboral, el crèdit, la fiabilitat o la conducta. No obstant això, l'article 36.2 RLOPD preveu i regula uns supòsits en els quals els afectats es poden veure sotmesos a una d'aquestes decisions.

El responsable del fitxer o tractament que accedeixi a la sol·licitud d'oposició "haurà d'excloure del tractament les dades relatives a la persona afectada que exerciti el seu dret d'oposició, o denegar motivadament la sol·licitud de la persona interessada en el termini previst en l'apartat 2 d'aquest article" (art. 35.3 RLOPD).

3.7.5. Reclamació de tutela de drets

En aquells casos en els quals l'exercici dels drets ARCO hagi donat un resultat infructuós per l'oposició i les reticències del responsable del fitxer o de l'encarregat del tractament (denegació total, denegació parcial o absència de resposta), l'article 18.2 LOPD preveu que la persona interessada pugui posar

aquest fet en coneixement de l'AEPD o, si escau, de l'organisme competent de cada comunitat autònoma, que s'haurà d'assegurar de la procedència o improcedència de la denegació.

En aquests casos, la LOPD preveu un procediment de tutela dels drets que es desplega en els articles 117 a 119 RLOPD, encara que aquest Reglament estableix que es tracta d'un procediment de l'AEPD, pel qual les autoritats de control autonòmiques haurien de disposar dels seus propis procediments o aplicar per analogia els de l'AEPD. Aquest procediment no té una naturalesa sancionadora, sinó reparadora del dret de la persona afectada.

Contra la resolució definitiva de l'AEPD escau la interposició d'un recurs contenciós administratiu (art. 18.4 LOPD) i, concretament, es pot recórrer en única instància davant de la Sala Contenciosa Administrativa de l'Audiència Nacional (DA 4a., apartat 5, de la Llei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa administrativa [LRJCA]).

A part de les reclamacions fetes per a fer efectius els drets que es reconeixen en la LOPD, els interessats que, com a conseqüència de l'incompliment del que disposa aquesta Llei, sofreixin danys o lesions en els seus béns o drets, tenen dret a ser indemnitzats (art. 19 LOPD).

3.8. Transferència internacional de dades

La transferència internacional de dades o el moviment internacional de dades es troben regulats en el títol V LOPD (art. 33 i 34) i en el títol VI RLOPD (art. 65 a 70), i comporta la transposició dels articles 25 i 26 de la Directiva 95/46.

La Directiva europea estableix el sistema de protecció de dades sobre la base del principi que les dades de caràcter personal constitueixen béns que s'integren dins del comerç. En conseqüència, els són aplicables la llibertat de circulació de béns, la llibertat de circulació de persones i la llibertat de circulació de serveis que s'estableixen com a llibertats bàsiques per a la consecució de les finalitats de la Unió Europea d'una manera idèntica a qualsevol altre bé objecte del comerç que es trobi en l'àmbit de la Unió.

Per tant, en sentit estricte, només hi ha transferència internacional de dades quan el país de destinació és un tercer estat; és a dir, un estat no membre de la Unió Europea (UE).

Lectura recomanada

J. Aparicio Salom (2009). *Estudio sobre la Ley orgánica de protección de datos de carácter personal*. Cizur Menor: Aranzadi.

Actualment, el moviment de dades entre països de la UE és lliure per aplicació de l'article 1.2 de la Directiva 95/46/CE. La Directiva va establir una regulació detallada mínima que pot ser superada per les legislacions nacionals, però que no serveix per a justificar qualsevol obstacle per a la lliure transmissió de dades entre els països integrants de la UE. L'estàndard de protecció de la Directiva es considera suficient i cap estat no pot invocar una protecció superior o sotmetre a autorització la transferència a organitzacions establertes al territori d'alguns

dels seus socis. Per contra, transferir dades a països amb menys protecció que la de la Directiva comporta una violació de la norma comunitària i, per tant, de les legislacions nacionals. En conseqüència, doncs, és susceptible de sanció.

Cal tenir en compte, també, que les transferències internacionals de dades no poden constituir una actuació abstracta, sinó que sempre hauran d'obeir a una causa concreta, adequada a la llei.

L'article 33.1 LOPD preveu que:

> "No es poden fer transferències temporals ni definitives de dades de caràcter personal que hagin estat objecte de tractament o hagin estat recollides per a sotmetre-les a aquest tractament amb destinació a països que no proporcionin un nivell de protecció equiparable al que dóna aquesta Llei, llevat que, a més d'haver-se observat el que s'hi disposa, s'obtingui una autorització prèvia del director de l'AEPD, que només la pot atorgar si s'obtenen garanties adequades".

L'AEPD ha d'avaluar el caràcter adequat de la protecció atenent una sèrie de circumstàncies previstes en l'article 33.2 LOPD. Tanmateix, s'ha de tenir en compte que les previsions de l'article 33 LOPD no són aplicables en els casos en què recull l'article 34 LOPD.

Basant-se en l'article 33.1 LOPD, la transferència internacional de dades es pot dur a terme:

a) Si el país destinatari de les dades ofereix un nivell de protecció equiparable al de la LOPD.

b) En defecte d'aquest nivell equiparable de protecció, sí que existeix l'autorització prèvia del director de l'AEPD, que només la pot atorgar si s'obtenen garanties adequades.

L'AEPD va publicar la Instrucció 1/2000, d'1 de desembre, relativa a les normes per les quals es regeixen els moviments internacionals de dades, a fi de donar unes pautes clares respecte a les transferències internacionals de dades. Aquesta Instrucció va ser objecte d'un recurs contenciós administratiu i la Sentència de l'Audiència Nacional, de 15 de març de 2002, va anul·lar determinades normes d'aquesta Instrucció que establien una sèrie de regles de verificació per a poder fer transferències internacionals de dades de caràcter personal que eren aplicables a tot tipus de transferències internacionals, sense distingir les que necessiten autorització prèvia de les que no la necessiten, encara que el marge d'actuació de l'AEPD en un cas i en l'altre és molt diferent.

Anul·lació de determinades normes de la Instrucció 1/2000 sobre els moviments internacionals de dades

Concretament, l'apartat 2 de la norma tercera i la norma sisena –si bé només perquè pretenien estendre'n l'aplicació a les transferències internacionals de dades compreses en els supòsits d'excepció de l'article 34 LOPD–, i també es va anul·lar l'apartat 1 de la norma quarta.

En tot cas, el RLOPD fa la distinció següent:

a) Supòsits en els quals es necessita l'autorització per a poder fer una transferència internacional de dades

Cal demanar una autorització que permeti fer la transferència i que s'atorga si es considera que el nivell de protecció del país al qual es fa l'exportació (destinatari de les dades) és adequat (art. 25.1 de la Directiva, 33 LOPD i 70 RLOPD).

Si no hi ha una declaració del director de l'AEPD o de la Comissió Europea que el nivell de protecció és adequat, s'haurà de sol·licitar al director de l'AEPD una autorització per a poder fer la transferència internacional (art. 70.1 RLOPD). L'autorització per a poder fer la transferència s'ha de tramitar d'acord amb el procediment establert en la secció primera del capítol V del títol IX de l'RLOPD.

b) Supòsits específics d'autorització: la solució contractual i les *binding corporate rules* (BCR)

S'atorga l'autorització si s'aporta un contracte per escrit, formalitzat entre l'exportador i l'importador, en el qual constin les garanties necessàries de respecte a la protecció de la vida privada dels afectats i als seus drets i a llibertats fonamentals i se'n garanteixi l'exercici dels drets respectius (art. 70.2 RLOPD).

L'article 70.2 RLOPD preveu que

> "A aquest efecte, es considera que estableixen les garanties adequades els contractes que se subscriguin d'acord amb el previst en 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, o del que disposin les decisions de la Comissió que compleixin l'establert en l'article 26.4 de la Directiva 95/46/CE".

L'AEPD, seguint el que preveu l'article 26.2 de la Directiva i la posició adoptada pel Grup de Protecció de Dades creat per la Directiva, ja havia admès la solució contractual com a instrument que permetia al responsable del tractament oferir les garanties adequades en transmetre dades fora dels països de la UE i, per tant, fora de l'àmbit d'aplicació de la Directiva i del marc general del dret comunitari.

La regulació contractual ha de preveure tots els principis bàsics de la protecció de dades i ha de fixar minuciosament la finalitat, els mitjans i les condicions del tractament de les dades transferides i també la manera com caldrà aplicar els principis bàsics de la protecció de dades. Cal tenir en compte expressament la prohibició de cessió a terceres persones no vinculades pel contracte.

En el supòsit que hi hagi BCR, segons l'article 70.4 RLOPD, l'autorització per a la transferència internacional de dades al si de grups multinacionals d'empreses també es pot atorgar quan aquests hagin adoptat normes o regles internes en les quals constin les garanties necessàries de respecte a la protecció de la vida privada i el dret fonamental a la protecció de dades dels afectats i es garanteixi, així mateix, el compliment dels principis i l'exercici dels drets reconeguts en la LOPD i el RLOPD.

c) Supòsits en els quals no es necessita autorització per a poder fer una transferència

- Quan es considera que l'estat en el qual es troba l'importador (país de destinació de les dades) proporciona un nivell adequat de protecció (art. 33.1 LOPD i 25.1 Directiva) i així ho ha declarat l'AEPD (art. 33.2 LOPD i 67 RLOPD) o la Comissió (art. 25.6 Directiva, 34.k LOPD i 68 RLOPD).

El caràcter adequat de protecció que ofereix el país de destinació s'avalua en funció dels paràmetres que estableixen els articles 25.2 Directiva, 33.2 LOPD i 67.1 RLOPD.

D'acord amb el que preveu l'article 25.6 de la Directiva, la Comissió ha reconegut Suïssa, Hongria, el Canadà, l'Argentina, Guernsey i l'illa de Man, els principis de port segur (*safe harbour*) per a la protecció de la vida privada. Atès el diferent nivell de protecció de les dades de caràcter personal entre els Estats Units i Europa, finalment es va arribar a l'Acord de port segur amb els Estats Units d'Amèrica, segons el qual la UE consent el flux de dades cap a companyies que voluntàriament acceptin un conjunt de principis i pràctiques definits pel Ministeri de Comerç dels Estats Units. Aquest òrgan és l'autoritat que exigeix el compliment dels principis a les organitzacions que s'acullen al *safe harbour* amb relació al tractament de les dades subministrades.

Les decisions adoptades que autoritzen la transferència internacional de dades suposen que les dades de caràcter personal poden circular des dels estats de la Unió Europea cap als estats en els quals ha recaigut una de les decisions citades sense que sigui necessari cap altre requisit.

En l'àmbit estatal, a fi de saber quins països considerats destinacions adequades l'AEPD de cara a l'exportació de dades de caràcter personal, l'RLOPD estableix que s'han de publicar en el BOE les resolucions del director de l'AEPD que acordin que un determinat país proporciona un nivell adequat de protecció, i aquesta llista s'ha de publicar i mantenir actualitzada a partir de mitjans informàtics o telemàtics (art. 67 RLOPD).

- Quan ocorren els supòsits dels articles 34 LOPD i 26.1 Directiva 95/46/CE.

Tant la Directiva com la LOPD recullen una sèrie de supòsits en els quals no és necessària l'autorització prèvia. La LOPD preveu que no fa falta l'autorització (art. 34.k LOPD) "quan la transferència tingui com a destinació un estat membre de la UE, o un estat respecte del qual la Comissió de la Comunitat Europea, en l'exercici de les seves competències, hagi declarat que garanteix un nivell de protecció adequat".

Ara bé, seguint Aparicio Salom, el supòsit de destinació de la transferència a un estat membre de la UE en rigor no és un supòsit de transferència internacional de dades, per la qual cosa, no és que s'apliqui l'excepció, és que no ens trobem davant d'un cas de transferència internacional de dades, sinó, en tot cas, davant d'una cessió.

Es requereixi o no autorització per a poder fer la transferència internacional, el que sí que és necessari per a qualsevol dels supòsits és que es notifiqui la transferència internacional de dades a l'AEPD a fi de procedir-ne a la inscripció en el Registre General de Protecció de Dades (art. 66.3 RLOPD).

Un altre aspecte que s'ha de tenir en compte és que el RLOPD preveu la possibilitat de declarar suspensions temporals de les transferències de dades cap a un importador ubicat en un tercer estat del qual s'hagi declarat l'existència d'un nivell adequat de protecció, quan es presentin determinades circumstàncies (art. 69 RLOPD).

3.9. Responsabilitat administrativa i responsabilitat civil

La LOPD estableix dos tipus diferents de responsabilitat: la responsabilitat administrativa (títol VII, articles 43-49 LOPD) i la responsabilitat civil (art. 19 LOPD).

3.9.1. La responsabilitat administrativa

La base de la responsabilitat administrativa es troba, no en la provocació d'un dany a una tercera persona, sinó en una infracció tipificada per l'ordenació i a què correspon una sanció pecuniària.

Com s'ha indicat, la LOPD estableix un règim de responsabilitat administrativa diferent segons si es tracta de fitxers de titularitat privada (art. 43.1 LOPD) o fitxers de titularitat pública (art. 43.2 LOPD). Respecte a aquests últims, a la pràctica, la responsabilitat és pràcticament inexistent. La potestat sancionadora correspon a l'AEPD (art. 37.g LOPD) i a les autoritats de control de les comunitats autònomes, segons correspongui (art. 41.1 LOPD, amb relació a l'article 37.g LOPD).

a) Fitxers de titularitat privada

L'article 43.1 LOPD estableix que els responsables dels fitxers i els encarregats dels tractaments estan subjectes al règim sancionador establert en la mateixa Llei.

La primera qüestió que cal remarcar és que l'article 43.1 LOPD fa referència al responsable del fitxer, mentre que en altres articles de la LOPD es fa referència al responsable del fitxer o del tractament, com en l'article 3.d LOPD. Aquests dos rols poden recaure en una mateixa persona, però pot no ser així. Tanma-

teix, en la mesura que aquests dos termes apareixen com a sinònims en la definició que proporciona l'article 3.d LOPD, la responsabilitat establerta en l'article 41 LOPD ha de ser aplicable tant al responsable del tractament com al responsable del fitxer.

A fi d'identificar aquest subjecte, l'element clau és l'exercici del poder decisori sobre la finalitat, el contingut i l'ús del tractament.

L'article 5.1.q RLOPD proporciona una definició de *responsable del fitxer o del tractament* similar a la de la LOPD, si bé afegeix "tot i que no el faci materialment". Per tant, d'una manera clara, l'element primordial és prendre una iniciativa, marcar-ne els criteris i les directrius.

Tot i així, l'exercici del poder decisori es pot desenvolupar en diferents moments: en el moment de la creació del fitxer i en el moment del tractament de les dades, i els subjectes protagonistes d'aquests dos moments poden no coincidir.

Segons Grimalt, ha de ser considerat com a responsable qui exerceix el control en el moment del tractament de les dades, és a dir, qui efectivament decideix sobre la finalitat, l'ús i el contingut concrets del fitxer.

Lectura recomanada

P. Grimalt Servera (1999). *La responsabilidad civil*. Granada: Comares.

Aquest autor fonamenta la seva opinió principalment en dos arguments:

- El tractament de dades és una activitat dinàmica que no es pot analitzar només en el moment de la seva creació, sinó que se n'ha de tenir en compte l'evolució.

- Des del punt de vista de la responsabilitat administrativa, no és correcte fer responsable un subjecte que no ha pres les decisions sobre la conducta objecte de sanció. Des del punt de vista de la responsabilitat civil, tampoc no sembla adequat fer recaure la responsabilitat en un subjecte que no té facultat decisòria.

Respecte a l'altre subjecte esmentat en l'article 43.1 LOPD –l'encarregat del tractament–, l'article 3.g LOPD el defineix com "la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que, només o juntament amb d'altres, tracta dades personals per compte del responsable del tractament".

Grimalt assenyala que, com es pot deduir de la definició, no es tracta d'un empleat del responsable del fitxer. Entre l'encarregat i el responsable sembla que hi hagi un contracte d'obra o de prestació de serveis. La mateixa opinió manifesta Vizcaíno, que indica que l'encarregat del tractament és una tercera persona que tracta les dades personals seguint les instruccions del responsable, si bé no sota la dependència o l'autoritat d'aquest des del punt de vista laboral.

Lectura recomanada

M. Vizcaíno Calderón (2001). *Comentarios a la Ley orgánica de protección de datos de carácter personal* (pàg. 83-84). Madrid: Civitas.

Respecte a les conductes susceptibles de sanció, estan descrites en l'article 44 LOPD i es classifiquen en tres nivells: infraccions lleus, infraccions greus i infraccions molt greus. Les sancions es troben regulades en l'article 45 LOPD.

Article 45 LOPD

La Sotssecretaria del Ministeri de Justícia va donar publicitat, mitjançant la Resolució, d'11 de desembre de 2001, a la conversió a euros dels valors corresponents a les sancions establertes en l'article 45 LOPD (BOE, núm. 303, de 19 de desembre de 2001).

En l'article 47 LOPD es regulen els terminis de prescripció de les infraccions i l'article 48 LOPD remet al desplegament reglamentari per tal d'establir el procediment sancionador. Aquest procediment és regulat pel RLOPD, títol IX ("Procediments tramitats per l'AEPD"), capítol III ("Procediments relatius a l'exercici de la potestat sancionadora"), articles 120-129.

L'article 82 de la Llei 62/2003, de 30 de desembre, de mesures fiscals, administratives i de l'ordre social va afegir en l'article 48 LOPD un paràgraf nou que establia la durada màxima de sis mesos per als procediments sancionadors tramitats per l'AEPD.

En determinats casos, davant d'una infracció molt greu, el director de l'AEPD pot procedir a la immobilització de fitxers. A més d'exercir la potestat sancionadora, pot requerir els responsables de fitxers de titularitat pública o privada la cessació en la utilització o cessió il·lícita de les dades. Si el requeriment és desatès, l'AEPD pot, mitjançant una resolució motivada, immobilitzar aquests fitxers per tal de restaurar els drets de les persones afectades (art. 49 LOPD i 121 RLOPD).

b) Fitxers de titularitat pública

L'article 43.2 LOPD estableix que si es tracta de fitxers els responsables dels quals són les administracions públiques, cal tenir en compte, quant al procediment i a les sancions, el que disposa l'article 46 LOPD. Aquest últim precepte preveu que, en els supòsits en els quals les infraccions es cometin en fitxers dels quals siguin responsables les administracions públiques, el director de l'AEPD ha de dictar una resolució que estableixi les mesures que correspongui adoptar que cessin o es corregeixin els efectes de la infracció. Aquesta resolució s'ha de comunicar a les diferents persones involucrades, entre les quals destaca l'òrgan de què depèn jeràrquicament el responsable del fitxer (art. 46.1 LOPD). Així mateix, el director de l'AEPD també pot proposar la iniciació d'actuacions disciplinàries, si escaigués. El procediment i les sancions que s'apliquin són els establerts en la legislació sobre règim disciplinari de les administracions públiques (art. 46.2 LOPD).

3.9.2. La responsabilitat civil

La finalitat de la responsabilitat civil, a diferència de l'administrativa, és reparar els danys causats a tercers. En la mesura que responsabilitat civil i responsabilitat administrativa obeeixen a finalitats diferents, es poden presentar les dues, o bé pot existir l'una sense l'altra.

La responsabilitat civil prevista en la LOPD resulta aplicable en els casos en els quals el responsable del fitxer o l'encarregat del tractament incompleixin el previst en la LOPD i causin un dany a la persona afectada (art. 19.1 LOPD).

Grimalt, referint-se a l'article 17.3 LORTAD, la redacció del qual és pràcticament igual que la de l'article 19.1 LOPD en aquest aspecte, estableix el següent:

> "[...] el legislador fa dependre el règim de responsabilitat civil d'un incompliment de l'estatut jurídic del responsable del fitxer; no vincula el deure de reparar el dany a la mera existència d'un tractament [...]; cal que es pugui imputar al responsable un incompliment i que se'n derivi el dany."

Lectura recomanada

P. Grimalt Servera (1999). *La responsabilidad civil en el tratamiento automatizado de datos de carácter personal* (pàg. 147). Granada: Comares.

Es tracta d'una responsabilitat de naturalesa objectiva; és a dir, la culpabilitat del responsable del fitxer o de l'encarregat del tractament és irrellevant. Quant a qui ostenta la qualitat de responsable i qui la d'encarregat, ens remetem a l'apartat anterior, relatiu a la responsabilitat administrativa.

L'aplicació de l'article 19 LOPD correspon a aquells supòsits en els quals s'hagi lesionat algun dret fonamental o llibertat pública, en la mesura que la LOPD tutela aquests drets. És dubtós si, en cas que es produeixi només un dany econòmic, sense vulneració dels drets fonamentals tutelats per la LOPD, resulta aplicable l'article 19 LOPD. En aquest cas, el rescabalament s'hauria d'articular per mitjà de les regles generals de la responsabilitat civil contingudes en el Codi civil.

Bibliografia

Aparicio Salom, J. (2009). *Estudio sobre la ley orgánica de protección de datos de carácter personal*. Cizur Menor: Aranzadi.

Díez-Picazo Giménez, L. M. (2005). *Sistema de derechos fundamentales*. Madrid: Thomson Civitas.

Díez-Picazo, L. M.; Ponce De León, L. (2007). *Fundamentos del derecho civil patrimonial. Vol. I.: Introducción: Teoría del contrato* (6a. ed.). Madrid: Thomson Civitas.

Goñi Sein, J. L. (2007). *La videovigilància empresarial y la protección de datos personales: Estudios de protección de datos*. Madrid: Civitas.

Grimalt Servera, P. (1999). *La responsabilidad civil en el tratamiento automatizado de datos personales*. Granada: Comares.

Guerrero Picó, M. C. (2006). *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*. Cizur Menor: Aranzadi.

Marí, J.; Vilasau, M. (coord.) (2008). *El Reglament de protecció de dades: aspectes clau*. Barcelona: UOC.

Martínez Martínez, R. (2001). *Tecnologías de la información, policía y Constitución*. València: Tirant lo Blanch.

Martínez Martínez, R. i altres (2008). *Comentarios al Reglamento de desarrollo de la LOPD*. València: Tirant lo Blanch.

Miguel Asensio, P. A. de (2002). *Derecho privado de Internet* (3a. ed.). Madrid: Civitas.

Miralles Miravet, S.; Baches Opi, S. (2002). "La cesión de datos de carácter personal: análisis de la legislación vigente y su aplicación a algunos supuestos prácticos". *La Ley* (vol. XXII, núm. 5306).

Oliver Lalana, D. (2002). "El derecho fundamental «virtual» a la protección de datos. Tecnología transparente y normas privadas". *La Ley* (núm. 5, pàg. 1539-1546).

Ribas Alejandro, J. (2000). "Riesgos legales en Internet. Especial referencia a la protección de datos personales". A: J. M. Cendoya Méndez de Vigo (coord.). *Derecho de Internet: Contratación electrónica y firma digital*. Cizur Menor: Aranzadi.

Rodríguez Casal, C.; Loza Corera, M. (2002). "Protección de la privacidad. Aproximación al *opt-in/opt-out*". *Revista de la Contratación Electrónica* (núm. 23, pàg. 3-18).

Roig, A. de A. (2002). "Protección de datos y derecho de las telecomunicaciones". A: J. Cremades; M. Á. Fernández-Ordóñez; R. Illescas. *Régimen jurídico de Internet* (pàg. 201-228). Madrid: La Ley.

Suñé Llinás, E. (2000). "Introducción y protección de datos personales". A: *Tratado de derecho informático* (vol. I, 2a. ed.). Madrid: Universidad Complutense, Facultad de Derecho, Servicio de Publicaciones / Instituto de Español de Informática y Derecho.

Téllez Aguilera, A. (2001). *Nuevas tecnologías y protección de datos: Estudio sistemático de la Ley orgánica 15/1999* (pàg. 150). Madrid: Edisofer.

Vizcaíno Calderón, M. (2001). *Comentarios a la Ley orgánica de protección de datos de carácter personal* (1a. ed.). Madrid: Civitas.