

# La protecció de dades personals a l'administració pública

Agustí Cerrillo i Martínez

PID\_00210703



*Els textos i imatges publicats en aquesta obra estan subjectes –llevat que s'indiqui el contrari– a una llicència de Reconeixement-NoComercial-SenseObraDerivada (BY-NC-ND) v.3.0 Espanya de Creative Commons. Podeu copiar-los, distribuir-los i transmetre'ls públicament sempre que en citeu l'autor i la font (FUOC. Fundació per a la Universitat Oberta de Catalunya), no en feu un ús comercial i no en feu obra derivada. La llicència completa es pot consultar a <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca>*

# Índex

<b>Introducció.....</b>	<b>5</b>
<b>Objectius.....</b>	<b>6</b>
<b>1. La regulació de la protecció de dades personals.....</b>	<b>7</b>
<b>2. Les dades personals a l'administració pública.....</b>	<b>23</b>
<b>Bibliografia.....</b>	<b>25</b>



## **Introducció**

Les tecnologies de la informació i la comunicació estan suposant noves amenaces a les dades personals. A continuació es presentaran les mesures que el dret està adoptant per tal de poder protegir les dades de les persones enfront dels atacs que poden provenir d'Internet.

Aquesta introducció s'articularà en dos àmbits. D'una banda, en general, quin ha estat la regulació de la protecció de les dades personals. D'altra banda, quin és l'impacte del desenvolupament de l'administració electrònica en la protecció de les dades personals.

## **Objectius**

Els objectius d'aquest mòdul són:

- 1.** Conèixer la regulació de la protecció de dades personals.
- 2.** Analitzar els diferents usos dels mitjans electrònics en l'administració pública des de la perspectiva de la protecció de les dades personals.
- 3.** Valorar l'impacte de la protecció de dades personals en el desenvolupament de l'administració electrònica.

# 1. La regulació de la protecció de dades personals

## Lectura proposada

A. Troncoso Reigada (2008). "La administración electrónica y la protección de datos personales". *Revista Jurídica de Castilla y León*. <[http://www.navarra.es/NR/rdonlyres/E6188543-88F9-476F-8581-406069D3C0E7/188896/32\\_AdministracionelectronicayprotecciondedatosTronc.pdf](http://www.navarra.es/NR/rdonlyres/E6188543-88F9-476F-8581-406069D3C0E7/188896/32_AdministracionelectronicayprotecciondedatosTronc.pdf)>

## a) Quins són els perills de l'extensió de les tecnologies de la informació i la comunicació per a les persones?

La Constitució espanyola reconeix el dret a la intimitat, que implica, com ha reconegut el Tribunal Constitucional, l'existència d'un àmbit propi i reservat enfront de l'acció i coneixement dels altres, necessari per a mantenir una qualitat mínima de la vida humana. A més, també preveu el dret a la protecció de les dades de caràcter personal que garanteix als individus un poder de disposar-ne i controlar-les.

Pagar els impostos per Internet o omplir un formulari per a sol·licitar una subvenció a una administració pública són dues activitats que més enllà de posar en contacte un ciutadà amb una administració per complir un deure o aconseguir un bé o un servei, posen en circulació a Internet dades personals (nom i cognoms, adreça, número de document d'identitat, número de la targeta de crèdit o del compte corrent). En molts casos aquestes dades poden semblar insignificants o podem no donar-li importància perquè no les considerem secretes o que no afecten el que considerem que és la intimitat de cadascú.

La utilització dels mitjans electrònics pot facilitar la vulneració de la intimitat de les persones. Les TIC permeten accedir i agregar dades personals disperses que d'aquesta manera faciliten un perfil de la persona afectada, la qual cosa era difícilment realitzable, o tenia costos molt elevats, sense utilitzar-les. També permeten poder conèixer les activitats realitzades en navegar per Internet, si es visita una pàgina o una altra o si es compra un producte o un altre. Tot això sense que la persona afectada en tingui coneixement i sense deixar cap rastre. D'aquesta manera, no pot fer cap control sobre aquestes dades ni sobre l'ús que se'n fa.

D'aquesta manera, per exemple, es pot arribar a la situació en què a partir dels pagaments que es fan actualment mitjançant la targeta de crèdit, fàcilment es pot obtenir una llista dels productes adquirits que doni idea del perfil de client que és, cosa molt interessant per a moltes empreses que volen saber quines són les preferències de clients potencials.

Aquesta situació ha estat clarament descrita en la STC 292/2000, de 30 de novembre, en afirmar el següent:

“Sense necessitat d'exposar de manera detallada les àmplies possibilitats que la informàtica ofereix tant per recollir com per comunicar dades personals ni els indubtables riscos que això pot comportar, ja que una persona pot ignorar no solament quines són les dades que el concerneixen que estan recollides en un fitxer sinó també si han estat traslladades a un altre i amb quina finalitat, n'hi ha prou d'indicar tots dos extrems per a comprendre que el dret fonamental a la intimitat (art. 18.1 CE) no aporti per si sol una protecció suficient davant d'aquesta nova realitat derivada del progrés tecnològic”.

Davant els riscos que la generalització de l'ús de les TIC pot suposar per a la intimitat de les persones, s'han adoptat diferents regulacions que tenen per objecte establir normes per a regular el tractament de dades personals i també s'han creat autoritats de control del compliment d'aquestes normes.

L'article 18.4 CE estableix que la “lleï limitarà l'ús de la informàtica per garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets”.

El Tribunal Constitucional ha reconegut l'existència d'un dret a l'autodeterminació informativa o d'una llibertat informàtica. Aquest dret va ser reconegut per primera vegada pel Tribunal Constitucional alemany en la sentència de 15 de desembre de 1983 sobre la Llei del cens. En aquesta sentència el Tribunal Constitucional alemany va considerar el dret a l'autodeterminació informativa sobre la base del dret a l'autodeterminació de la persona i va identificar que aquest nou dret que implica que cada individu pot decidir bàsicament per si mateix quan i dins de quins límits és procedent revelar situacions referents a la pròpia vida. Per al Tribunal Constitucional alemany, el lliure desenvolupament de la personalitat pressuposa, en les condicions modernes de l'elaboració de dades, la protecció de l'individu contra la recollida, l'emmagatzematge, la utilització i la transmissió il·limitades de les dades referents a la persona. Així, tal com afirma en el fonament jurídic segon:

[...] en la clau de volta de l'ordenament de la Llei fonamental es troba el valor i la dignitat de la persona, que actua amb lliure autodeterminació com a membre d'una societat lliure. El dret general de la personalitat inclou la facultat de l'individu, derivada de l'autodeterminació, de decidir bàsicament per si mateix quan i dins de quins límits és procedent revelar situacions referents a la pròpia vida: la lliure eclosió de la personalitat pressuposa en les condicions modernes de l'elaboració de dades de protecció de l'individu contra la recollida, l'emmagatzemament, la utilització i la transmissió il·limitada de les dades que concerneixen la persona.

El dret fonamental garanteix, en efecte, la facultat de l'individu de decidir bàsicament per si sol sobre la difusió i utilització de les seves dades personals<sup>1</sup>”.

De totes maneres, cal posar de manifest que el dret a l'autodeterminació informativa no és un dret absolut, per la qual cosa ha de ser ponderat amb altres drets o interessos que en un moment donat es consideren de prioritària atenció.

“Les limitacions d'aquest dret a l'«autodeterminació informativa» solament són admissibles en el marc d'un interès general superior i necessiten un fonament legal basat en la Constitució que han de correspondre a l'imperatiu de claredat normativa inherent a l'estat de dret<sup>2</sup>”.

(1) <http://www.informatica-juridica.com/jurisprudencia/alemania.asp>

(2) STC alemany de 15 de desembre de 1983.



## b) Quin és el contingut que el Tribunal Constitucional ha donat al dret a la protecció de les dades personals?

La jurisprudència del Tribunal Constitucional ha permès delimitar el contingut del dret previst a l'article 18.4 CE. Així, per exemple, la STC 254/1993, de 20 de juliol:

“En efecte, s'ha de tenir present, com ja s'anticipava en la decisió d'aquest Tribunal que s'acaba d'esmentar, que el dret fonamental al qual fem referència garanteix a la persona un poder de control i disposició sobre les seves dades personals. Atès que confereix al seu titular un feix de facultats que són elements essencials del dret fonamental a la protecció de les dades personals, integrat pels drets que corresponen a l'afectat a consentir que es recullin i utilitzin les seves dades personals i a conèixer-les. I per fer efectiu aquest contingut, el dret a ser informat de qui posseeix les seves dades personals i amb quina finalitat, així com el dret a oposar-se a aquesta possessió i ús exigint a qui correspongui que s'hi posi fi.

En suma, el dret fonamental comprèn un conjunt de drets que el ciutadà pot exercir davant dels qui siguin titulars, públics o privats, de fitxers de dades personals, partint del coneixement d'aquests fitxers i del seu contingut, ús i destinació, pel registre d'aquests. De manera que és en aquests fitxers on s'han de projectar, en última instància, les mesures destinades a la salvaguarda del dret fonamental aquí considerat per part de les administracions públiques competents”.

## c) Quines són les relacions entre el dret a la intimitat i el dret a la protecció de les dades personals?

La STC 292/2000, de 30 de novembre, permet distingir clarament entre el dret a la intimitat i el dret a l'autodeterminació informativa:

“6. La funció del dret fonamental a la intimitat de l'article 18.1 CE és protegir davant de qualsevol invasió que es pugui realitzar en aquell àmbit de la vida personal i familiar que la persona desitja 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 destinació, amb el propòsit d'impedir-ne el tràfic il·lícit i lesiu per a la dignitat i dret de l'afectat. En conclusió, 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 degudes garanties; i també el deure de prevenir els riscos que es puguin derivar de l'accés o divulgació indegudes d'aquesta informació. Però aquest poder de disposició sobre les pròpies dades personals no val res si l'afectat desconeix quines dades posseeixen tercers, qui les posseeixen, i amb quina finalitat.

D'aquesta manera, l'objecte de protecció del dret fonamental a la protecció de dades no es redueix solament a les dades íntimes de la persona, sinó a qualsevol tipus de dada personal, tant si és íntima com si no, el coneixement o ús de la qual per tercers pugui afectar els seus drets, tant si són fonamentals com si no, perquè el seu objecte no és solament la intimitat individual, que per a això hi és la protecció que l'article 18.1 CE atorga, sinó les dades de caràcter personal<sup>3</sup>”.

D'acord amb el TC, la distinció entre els dos drets es concreta, d'una banda, per l'objecte que té i, d'una altra, pel contingut.

<sup>(3)</sup>Vegeu també la STC 143/1994, de 9 de maig, FJ 7.

Pel que fa a l'objecte, l'article 18.4 CE és més ampli que el dret a la intimitat ja que no es limita a les dades íntimes de les persones, sinó que estén la garantia a qualsevol tipus de dades personals, tant íntimes com no, el coneixement de les quals per tercers pugui afectar els drets de la persona.

Pel que fa al contingut, l'article 18.1 CE confereix al titular un poder jurídic per imposar a tercers el deure d'abstenir-se de tota intromissió en l'esfera íntima de la persona i la prohibició de fer ús del que hagi estat conegut mitjançant una intromissió i, en canvi, el dret de protecció de dades atribueix al titular un conjunt de facultats consistent en diferents poders jurídics l'exercici dels quals imposa a tercers deures jurídics, els quals serveixen a la funció que realitza el dret a la protecció de dades: garantir a la persona un poder sobre les seves dades personals.

#### **d) Com s'ha regulat la protecció de les dades personals?**

El moviment regulador té l'origen en l'àmbit estatal. La primera llei sobre protecció de dades va ser aprovada en el *Land* alemany de Hessen el 1970. Posteriorment, altres estats com Suècia, els Estats Units, Nova Zelanda, el Canadà i gran part dels països europeus s'han dotat d'instruments legislatius en aquesta matèria.

Bona part d'aquest moviment ha tingut l'origen en les regulacions promogudes internacionalment. En primera instància el Conveni 108 del Consell d'Europa, de 28 de gener de 1981, de protecció de les persones en relació amb el tractament automatitzat de les dades de caràcter personal. L'objectiu del conveni és assegurar al territori dels estats signants que es respecti el dret de cada individu, independentment de la nacionalitat o residència que tingui, a la privacitat respecte al procés automatitzat de dades personals que es refereixen a ell.

Posteriorment, en l'àmbit comunitari, s'ha aprovat la Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre, relativa a la protecció de les persones físiques i la Directiva 2002/58/CE del Parlament Europeu i del Consell, de 12 de juliol, relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques. El maig de 2003, es va adoptar un informe sobre l'aplicació de la Directiva 95/46 d'acord amb el que estableix l'article 33. En aquest informe es constata que la Directiva 95/46 havia assolit l'objectiu d'atorgar una protecció suficient de la privacitat i que al mateix temps havia facilitat la transferència de dades a la Unió Europea. No obstant això, la tardança en la implementació de la Directiva per part d'alguns estats membres i també les diferències en la seva transposició han motivat que l'economia europea no s'hagi beneficiat completament de la Directiva<sup>4</sup>.

<sup>(4)</sup>Vegeu l'informe a: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:ES:NOT>.

## Exemple

Tal com recorda la Sentència del Tribunal de Justícia de la Unió Europea de 20 de maig de 2003 en els assumptes acumulats C-465/00, C-138/01 i C-139/01, la Directiva 95/46 “s’ha adoptat sobre la base de l’article 100 A del Tractat, té per objecte garantir la lliure circulació entre estats membres de les dades personals mitjançant l’harmonització de les normes nacionals que protegeixen les persones físiques pel que fa al tractament d’aquestes dades”. En efecte, l’article 1 d’aquesta Directiva, que defineix el seu objectiu, disposa, en l’apartat 2, que els estats membres no poden restringir ni prohibir la lliure circulació de dades personals entre els estats membres per motius relacionats amb la protecció de les llibertats i dels drets fonamentals de les persones físiques, i, en particular, del dret a la intimitat, pel que fa al tractament d’aquestes dades.

La legislació europea ha estat traslladada a l’ordenament jurídic espanyol mitjançant la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD) i, en determinats aspectes, per la Llei 34/2002, d’11 de juliol, de serveis de la societat de la informació (LSSI). La LOPD va derogar la Llei orgànica 5/1992, de 29 d’octubre, de regulació del tractament automatitzat de les dades de caràcter personal.

A més, tres comunitats autònomes han adoptat algunes normes sobre aquesta qüestió. La Comunitat de Madrid va ser la primera comunitat autònoma a aprovar una llei en aquesta matèria, en particular la Llei 8/2001, de 13 de juliol, de protecció de dades de caràcter personal en la Comunitat de Madrid, que té per objecte regular els fitxers de dades de caràcter personal i l’Agència de Protecció de Dades de la Comunitat de Madrid. Posteriorment, la Llei 5/2002, de 19 d’abril, de l’Agència Catalana de Protecció de Dades, que com es desprèn del seu títol crea i regula l’Agència Catalana de Protecció de Dades (en l’actualitat, Llei 32/2010, d’1 d’octubre, de l’Autoritat Catalana de Protecció de Dades). Finalment, el País Basc ha aprovat 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 amb l’objectiu de regular els fitxers de dades de caràcter personal creats o gestionats per la Comunitat Autònoma del País Basc, els òrgans forals dels territoris històrics i les administracions locals de la Comunitat Autònoma del País Basc i crear i regular l’Agència Basca de Protecció de Dades.

A més de totes aquestes normes que directament incideixen i tenen per objecte únic i específic la protecció de les dades de caràcter personal, s’ha de posar en relleu altres normes de caràcter general que incideixen en aquesta matèria. Són normes com el Codi penal i el Codi civil, o la Llei 34/2002, d’11 de juliol, de serveis de la societat de la informació i el comerç electrònic (LSSI), a la qual s’ha de fer particular esment.

També cal posar en relleu que en determinats àmbits s’ha optat per adoptar codis de conducta, és a dir, mecanismes d’autoregulació per part del mateix sector que impliquen que aquells que s’hi acullen s’obliguen a seguir les regles de conducta que s’hi estableixen. La LOPD preveu la possibilitat de formular codis tipus als responsables de fitxers, a través d’acords sectorials o mitjançant decisions d’empresa. En particular, l’article 32 LOPD preveu que els responsables de tractaments de titularitat pública i privada poden formular

codis que estableixin les condicions d'organització, règim de funcionament, procediments aplicables, normes de seguretat de l'entorn, programes o equips, obligacions dels implicats en el tractament i ús de la informació personal, així com les garanties per a l'exercici dels drets de les persones. Els codis tipus tenen el caràcter de codis deontològics o de bona pràctica professional i s'han de dipositar i inscriure en el Registre General de Protecció de Dades.

**e) Com es garanteix el compliment de la legislació sobre protecció de dades personals?**

L'Agència Espanyola de Protecció de Dades és un ens de dret públic amb personalitat jurídica pròpia i plena capacitat pública i privada que actua amb independència de les administracions públiques en l'exercici de les seves funcions. Entre les funcions destaquen:

- Vetllar pel compliment de la legislació sobre protecció de dades i controlar-ne l'aplicació, especialment pel que fa als drets d'informació, accés, rectificació, oposició i cancel·lació de dades.
- Atendre les peticions i reclamacions dels afectats.
- Emetre les autoritzacions que preveu la Llei, ordenar, en cas d'il·legalitat, el cessament en el tractament i la cancel·lació de les dades, exercir la potestat sancionadora, demanar l'ajuda i informació que necessiti.
- Informar dels projectes de normes de desplegament que incideixin en matèries de protecció de dades.

Per aconseguir aquests fins, la mateixa Llei reconeix tot un seguit de potestats com són les d'investigació i inspecció per a obtenir informació i, si escau, proves sobre els fets que contravinguin el que disposa la Llei, la potestat sancionadora, que l'Agència de Protecció de Dades ha d'exercir en els termes que preveu la Llei, la potestat de resolució de les reclamacions dels afectats per incompliment de les previsions d'aquesta Llei i la potestat normativa, cenyida en l'essencial a dictar les instruccions necessàries per a adequar els tractaments automatitzats als principis de la LOPD.

La STC 290/2000 és clara en definir el caràcter de les funcions de l'Agència Espanyola de Protecció de Dades:

En efecte, com que dóna compliment al mandat que conté l'article 18.4 CE, el legislador, sense excloure de cap manera el recurs últim als òrgans jurisdiccionalmentals per a la tutela dels drets individuals, com es determina en els apartats 2 a 5 de l'article 17 LORTAD, no ha volgut tanmateix que la protecció de dades personals davant l'ús de la informàtica es porti a terme exclusivament en la via judicial, això és, quan ja s'ha produït una lesió del dret fonamental. Al contrari, ha volgut que aquesta protecció es porti a terme mitjançant l'exercici per l'Agència de Protecció de Dades, amb caràcter bàsicament preventiu, de les funcions de control dels fitxers tant de titularitat pública com privada que la LORTAD li atribueix i, si escau, a través de les reclamacions dels afectats davant l'Agència de Protecció de Dades (art. 17.1), les quals provocaran la posterior actuació d'aquest òrgan.

En aquesta sentència els recurrents consideren que en limitar les competències autonòmiques als fitxers automatitzats de dades de caràcter personal creats o gestionats per elles es vulnerava el sistema de distribució de competències, ja que com a conseqüència d'aquesta limitació, correspon en exclusiva a un òrgan estatal, l'Agència de Protecció de Dades, l'execució de la Llei i l'exercici de les funcions interventores i sancionadores que s'hi preveuen respecte de la resta de fitxers automatitzats. El Tribunal Constitucional considera que "és la garantia dels drets fonamentals exigida per la Constitució així com la de la igualtat de tots els espanyols en el seu gaudi la que en aquest cas justifica que l'Agència de Protecció de Dades i el Registre Central de Protecció de Dades pot exercir les funcions i potestats a què abans s'ha fet referència respecte als fitxers informatitzats que continguin dades personals i que siguin de titularitat privada radicats a Catalunya".

A Catalunya, l'any 2003 es va crear l'Agència Catalana de Protecció de Dades que, com recull la seva llei de creació, té per objecte vetllar pel respecte dels drets fonamentals i les llibertats públiques dels ciutadans en tot allò que faci referència a les operacions fetes mitjançant processos automatitzats o manuals de dades personals.

A Madrid, l'Agència de Protecció de Dades de la Comunitat de Madrid té com a finalitat garantir i protegir els drets fonamentals de les persones físiques respecte a l'honor i intimitat familiar i personal, pel que fa al tractament de les seves dades personals. Les seves competències versen sobre els fitxers de titularitat pública creats o gestionats per la Comunitat Autònoma de Madrid, ens que integren l'Administració local del seu àmbit territorial, universitats públiques i corporacions de dret públic representatives d'interessos econòmics i professionals d'aquella. Malgrat la intensa activitat desenvolupada des de la seva creació, l'Agència de Protecció de Dades de la Comunitat de Madrid va ser suprimida el 2012.

Al País Basc, l'Agència Basca de Protecció de Dades és un ens de dret públic, amb personalitat jurídica pròpia i plena capacitat pública i privada, que actua amb plena independència de les administracions públiques en l'exercici de les seves funcions, entre les quals destaquen vetllar pel compliment de la legislació sobre protecció de dades i controlar-ne l'aplicació i emetre les autoritzacions previstes en les lleis i reglaments.

## f) Què és una dada personal?

La primera qüestió que s'ha de delimitar és la relativa a què s'entén per *dada*. De la legislació espanyola de protecció de dades es poden exposar les següents consideracions de caràcter general. La LOPD, seguint la Directiva 95/46, parteix d'una definició àmplia de les dades personals: “qualsevol informació concernent a persones físiques identificades o identificables”.

Identificada o identificable és tota persona la identitat de la qual es pugui determinar, directament o indirectament, en particular mitjançant un número d'identificació o un o diversos elements específics, característics de la seva identitat física, fisiològica, psíquica, econòmica, cultural o social. En relació amb aquest concepte es plantegen alguns dubtes, entre els quals destaca si es poden considerar les persones jurídiques com a titulars dels drets reconeguts en la LOPD. Tenint en compte que l'article 18.4 CE es refereix als ciutadans i que la Directiva 95/463 fa referència a la protecció de les persones físiques, sembla que s'ha de concloure en sentit negatiu. No obstant això, si les dades referides a una persona jurídica es poden atribuir a una persona física concreta, encara que fossin tractades com a dades d'una persona jurídica, tindrien la consideració de dades de caràcter personal.

Les dades de caràcter personal no són únicament informació numèrica o alfanumèrica, sinó que també s'ha d'entendre que fan referència a la imatge, la veu, les empremtes dactilars o les dades biomètrics. Aquestes dades no han d'estar únicament en fitxers automatitzats. A diferència de la LORTAD, la LOPD considera que la norma és aplicable a les dades de caràcter personal registrades en suport físic.

L'ús de les noves tecnologies planteja si determinada informació pot considerar com a dada de caràcter personal. En particular, la pregunta seria si l'adreça de correu electrònic i l'adreça d'IP són dades de caràcter personal. Pel que fa a l'adreça de correu electrònic, si tenim en compte que per a considerar que estem davant una dada personal cal que hi hagi una vinculació entre la informació i la persona concreta, l'adreça de correu electrònic no s'hauria de considerar dada de caràcter personal mentre no hi hagi aquesta relació. Pel que fa a l'adreça IP, l'Agència Espanyola de Protecció de Dades considera que és una dada de caràcter personal:

“Així doncs, encara 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, independentment del tipus d'accés, es consideren dades de caràcter personal i hi és aplicable la normativa sobre protecció de dades<sup>5</sup>”.

<sup>(5)</sup>Informe 327/03.

## g) Quins són els principis de la protecció de dades?

La LOPD estableix tot un seguit de principis:

**Qualitat de les dades.** Les dades personals han de ser adequades, pertinents i no excessives respecte a la finalitat per a la qual s'obtenen i han de ser exactes i actualitzades. Es tracta d'assegurar la veracitat i exactitud de les dades obtingudes i tractades. Com afirma la Sentència de la Sala Contenciosa Administrativa de l'Audiència Nacional, de 9 de març de 2001:

“Un dels principis que inspira la legislació sobre tractament automatitzat de dades de caràcter personal és el de qualitat de dades. Aquest principi implica, entre altres coses, que les dades siguin necessàries i pertinents per a la finalitat per a la qual s'hagin recollit o registrat (art. 4.5 de la LO 5/1992) i que siguin exactes i completes (art. 4.4 de la LO 5/1992). Per tant, si les dades han deixat de ser necessàries per a les finalitats per a les quals es van recollir o registrar o són inexactes, s'ha de procedir [...] a cancel·lar-les, sense necessitat de demanar-ho a l'afectat. I així s'infereix del mateix tenor literal dels articles 4.4 i 4.5 de la LO 5/1992, que utilitza l'expressió imperativa «han de ser cancel·lades» i sense condicionar-la a l'existència d'una sol·licitud prèvia de l'afectat. En suma, la norma estableix l'obligació del responsable del fitxer de procedir d'ofici i amb la deguda diligència a cancel·lar les dades inexactes o que han deixat de ser necessàries per a la finalitat del fitxer i sense necessitat de sol·licitud prèvia de l'afectat”.

**Consentiment.** El tractament de les dades de caràcter personal requereix el consentiment inequívoc de l'interessat. La Sentència de la Secció Vuitena de la Sala Contenciosa Administrativa del Tribunal Superior de Justícia de Madrid, de 29 novembre de 1999, afirma sobre aquesta qüestió el següent:

“[...] El precepte estableix no solament l'ús de les dades sinó el tractament [...]. Doncs bé, aquest tractament ha de respectar, entre altres garanties previstes per la Llei, la que estableix l'article 6, apartats 1 i 2, que exigeixen per al tractament de les dades, el consentiment de l'afectat, consentiment que no és necessari quan les dades de caràcter personal es recullen de fonts accessibles al públic. La infracció d'aquesta garantia és la que s'imputa concretament a l'actora, establint-se ja des del plec de càrrecs que les dades no s'han obtingut amb el consentiment de l'interessat ni provenen de fonts accessibles al públic”.

Hi ha dades (ideologia, afiliació sindical, religió i creences) que tenen una protecció reforçada i que requereixen un consentiment exprés i per escrit. Altres dades (origen racional, salut o vida sexual) només poden ser recollides, tractades i cedides quan, per raons d'interès general, així ho disposi una llei o l'afectat ho consenti expressament.

En relació amb el principi del consentiment hi ha el de la plena informació de l'afectat, respecte al qual es pot portar a col·lació la Sentència de la Sala Contenciosa Administrativa de l'Audiència Nacional, de 15 de juny de 2001:

“En primer lloc, s'ha de tenir en compte que ens trobem davant la regulació del dret de la informació a la recollida de dades, dret importantíssim perquè és el que permet portar a terme l'exercici d'altres drets i així ho valora el text positiu en detallar-ne el contingut i establir l'exigència que aquest sigui exprés, precís i inequívoc. La rellevància del dret comporta que la seva exclusió requereixi el mandat exprés d'una norma, acollint una interpretació estricta, vedant-se la seva extensió mitjançant artificioses deduccions”.

**Seguretat de les dades.** D'acord amb l'article 9 LOPD, “el responsable del fitxer i, si s'escau, l'encarregat del tractament han d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no

autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposats, tant si provenen de l'acció humana o del medi físic o natural”.

**Secret en el tractament de les dades.** El responsable del fitxer i del tractament està obligat al secret professional. D'acord amb la Sentència de la Secció Novena de la Sala Contenciosa Administrativa del Tribunal Superior de Justícia de Madrid, de 3 de maig de 2001:

“[...] el deure de guardar secret de l'article 10 queda definit pel caràcter personal de la dada integrada en el fitxer, del secret de la qual només té facultat de disposició el subjecte afectat, ja que no en va el dret a la intimitat és un dret individual i no col·lectiu. Per això, és igualment il·lícita la comunicació a qualsevol tercer, amb independència de la relació que hi mantingui la persona a què es refereixi la informació. En aquest cas [...] la repercussió per a l'afectat de la divulgació de dades a tercers és summament subjectiva, de tal manera que, en el cas que ens ocupa, podria afectar més a la interessada la comunicació del seu deute al seu pare que a qualsevol altra persona”.

**Congruència i racionalitat en la seva utilització.** Així, l'article 11 LOPD estableix que “les dades de caràcter personal objecte del tractament només poden ser comunicades a un tercer per al compliment de finalitats directament relacionades amb les funcions legítimes del cedent i del cessionari amb el consentiment previ de l'interessat”.

#### **h) Quins són els drets de les persones respecte a les dades personals?**

Per tal de garantir el compliment d'aquests principis, la LOPD regula els drets dels titulars de les dades personals i els tractaments que es poden fer:

**Dret d'accés.** L'interessat té dret a sol·licitar i obtenir gratuïtament informació de les seves dades de caràcter personal sotmeses a tractament, l'origen de les dades i les comunicacions realitzades o que es prevegin fer. En la Sentència de la Secció Vuitena de la Sala Contenciosa Administrativa del Tribunal Superior de Justícia de Madrid, de 17 de maig de 2000, es va afirmar el següent:

“El dret d'accés és el dret a sol·licitar i obtenir informació de les dades de caràcter personal incloses en els fitxers automatitzats [...] I va ser precisament la falta de resposta de la petició d'informació del denunciant [...] en el termini d'un mes [...] la que va motivar la incoació d'un procediment de tutela del dret d'accés del denunciant, la finalitat del qual no era una altra que la de donar efectivitat a aquest dret [...] en no haver estat satisfet pel titular del fitxer [...]”.

**Dret de rectificació i cancel·lació.** Han de ser rectificades o cancel·lades, si s'escau, les dades de caràcter personal quan el tractament no s'ajusti al que disposa LOPD. En aquest sentit, la Sentència de la Secció Novena de la Sala Contenciosa Administrativa del Tribunal Superior de Justícia de Madrid, de 17 de juny de 1999, recull el següent:



“[...] el responsable del fitxer és el [...] que té l'obligació de fer efectiu el dret de rectificació i cancel·lació [...] La Instrucció 1/98 ha estat aclaridora, ja que imposa al responsable del fitxer l'obligació de prendre mesures per traslladar la sol·licitud que es faci de cancel·lació o rectificació, a l'entitat bancària subministradora de la dada, de manera que si no rep resposta en cinc dies, ha de procedir a la rectificació cautelar dels fitxers”.

**Dret d'oposició.** Es reconeix en dos preceptes de la LOPD, els articles 6.4 i 30.4. El primer reconeix el dret de l'interessat que tingui un interès legítim a oposar-se al tractament de les seves dades en aquells supòsits en què, d'acord amb el que preveu l'article 6.2, no calgui demanar-li el consentiment, i indica que “en els casos en què no sigui necessari el consentiment de l'afectat per al tractament de les dades de caràcter personal, i sempre que una llei no disposi el contrari, aquest pot oposar-se al seu tractament quan hi hagi motius fonamentats i legítims relatius a una situació personal concreta. En aquest supòsit, el responsable del fitxer ha d'excloure del tractament les dades relatives a l'afectat”.

El segon reconeix l'anomenat *dret d'opt-out*, o dret a no ser inclòs en les llistes obtingudes de fonts accessibles al públic i empleats amb fins de publicitat o prospecció comercial, i estableix que “els interessats tenen dret a oposar-se, amb la petició prèvia i sense despeses, al tractament de les dades que els concerneixin, cas en què han de ser donats de baixa del tractament i s'han de cancel·lar les informacions que sobre els interessats figurin en el tractament, amb la simple sol·licitud”.

La mateixa LOPD preveu algunes excepcions als drets anteriors. En particular, l'article 23 LOPD estableix, entre altres, que “els responsables dels fitxers que continguin les dades a què es refereixen els apartats 2, 3 i 4 de l'article anterior poden denegar l'accés, la rectificació o la cancel·lació en funció dels perills que es puguin derivar per a la defensa de l'Estat o la seguretat pública, la protecció dels drets i les llibertats de tercers o les necessitats de les investigacions que s'estiguin duent a terme”.

L'Agència Espanyola de Protecció de Dades és competent respecte a la tutela del dret d'accés que correspon a cada persona i deriva del seu dret a la privacitat de les seves dades de caràcter personal. Així, davant d'una denegació de l'exercici d'aquest dret, queda oberta la possibilitat de demanar aquesta tutela formulant la corresponent reclamació.

#### **i) Com es poden obtenir les dades?**

La LOPD preveu diferents mecanismes per a l'obtenció de les dades:

#### **Obtenció de dades del mateix interessat**

En primer lloc, l'obtenció pot ser a través de la persona que bé les ha facilitat directament o bé manifesta el consentiment exprés perquè siguin recollides amb una finalitat concreta i, per tant, no genèrica. El subministrament de dades pot ser voluntari o fruit d'una obligació legal (per exemple, les dades necessàries per a l'empadronament).

D'acord amb la LOPD, "les dades de caràcter personal objecte de tractament no es poden utilitzar per a finalitats incompatibles amb aquelles per a les quals hagin estat recollides". Per això, s'ha d'entendre que el consentiment es dona respecte a un tractament que té una finalitat concreta, no és un consentiment abstracte, sinó per a un o uns tractaments concrets. El consentiment ha de ser inequívoc a través d'una manifestació de voluntat, lliure, inequívoca, específica i informada, mitjançant la qual l'interessat consenti el tractament de les dades personals que el concerneixen.

Tal com s'ha observat anteriorment, hi ha determinats casos en què la LOPD exigeixen consentiment reforçat per tractar determinats dades a causa del caràcter especialment sensible que tenen. A més, en relació amb les dades sobre ideologia, religió o creences s'ha d'advertir l'interessat sobre el dret a no prestar el consentiment. És interessant posar en relleu que respecte a aquestes dades no cal el consentiment quan el tractament sigui necessari per a la prevenció o diagnòstic mèdics, la prestació d'assistència sanitària o tractaments mèdics o la gestió de serveis sanitaris o per salvaguardar l'interès vital de l'afectat o d'una altra persona, en cas que l'afectat estigui físicament o jurídicament incapacitat per a donar el consentiment.

Encara que s'hagi prestat el consentiment, aquest és revocable quan hi hagi una causa justificada i no se li atribueixen efectes retroactius.

La LOPD preveu algunes excepcions a la necessitat del consentiment. En primer lloc, 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. En segon lloc, quan es refereixin a les parts d'un contracte o precontracte d'una relació de negocis, laboral o administrativa i siguin necessàries per al seu manteniment o compliment. En tercer lloc, quan el tractament tingui per finalitat protegir un interès vital de l'interessat. I, en quart lloc, 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 del tercer a qui es comuniquin les dades, sempre que no es vulnerin els drets i llibertats fonamentals de l'interessat.

### **Obtenció de dades de fonts diferents de l'interessat**

L'obtenció de dades de fonts diferents de l'interessat pot ser a través de fonts accessibles al públic com per exemple, els censos promocionals, els repertoris telefònics o les llistes professionals o com a resultat de la cessió de dades personals de subjectes diferents de l'interessat.

Com a punt de partida en aquest supòsit cal portar a col·lació l'article 5.4 LOPD, que estableix que quan les dades no s'obtinguin de l'interessat cal informar-lo, de manera expressa, precisa i inequívoca, dins dels tres mesos següents al moment de registre de les dades, del contingut del tractament, procedència de les dades i de la resta d'aspectes que preveu la Llei.

D'acord amb la LOPD, són fonts accessibles al públic "els fitxers que poden ser consultats per qualsevol persona, sense que ho impedeixi una norma limitativa o sense altra exigència que, si s'escau, l'abonament d'una contraprestació". Tenen la consideració de fonts d'accés públic el cens promocional, els repertoris telefònics i les llistes de persones pertanyents a grups de professionals que continguin únicament les dades de nom, títol, professió, activitat, grau acadèmic, direcció i indicació de la seva pertinença al públic. També tenen la consideració de fonts de caràcter públic, els diaris i butlletins oficials i els mitjans de comunicació. Tot i que les dades s'obtinguin d'una font no es poden sotmetre a qualsevol tipus de tractament. Cal que el tractament de les dades sigui necessari per a la satisfacció d'un interès legítim del responsable del fitxer o del tercer a qui es comuniquin les dades i que es compleixi la condició de no vulnerar els drets i llibertats fonamentals de l'afectat.

Per a la cessió de dades és necessari que aquestes serveixin per al compliment de finalitats directament relacionades amb les funcions legítimes del cedent i del cessionari i el consentiment previ de l'interessat. No obstant això, estan previstes diferents excepcions a la regla del consentiment previ. La comunicació de dades entre administracions públiques estava prevista en l'article 21 LOPD, que va ser declarat inconstitucional per la STC 292/2000, de 30 de novembre.

#### **j) Com s'han de crear els fitxers de dades personals?**

Tant les administracions públiques com els particulars poden crear fitxers que continguin dades personals. Els requisits en un cas i un altre són diferents però tenen en comú la necessitat d'inscriure el fitxer en el Registre General de Protecció de Dades creat a aquest efecte a l'Agència Espanyola de Protecció de Dades.

**Els 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. Només es poden crear, modificar o suprimir per mitjà d'una disposició general publicada al BOE o al diari oficial corresponent. Un cop

creat el fitxer, l'Administració o l'organisme responsable ho ha de comunicar a l'Agència Espanyola de Protecció de Dades per a la inscripció en el Registre General de Protecció de Dades.

La LOPD regula la recollida i tractament de dades per a finalitats policials sense el consentiment de les persones afectades. Respecte als fitxers de les forces i cossos de seguretat s'estableixen una sèrie d'excepcions als drets d'accés, rectificació i cancel·lació i també la limitació de drets com el d'informació a l'afectat.

**Els fitxers de titularitat privada.** D'acord amb la LOPD, són fitxers de titularitat privada els que continguin dades de caràcter personal quan, de forma acumulativa, sigui necessari per a la consecució de l'activitat o objecte legítim de la persona, empresa o entitat titular i es respectin les garanties que la LOPD estableix per a la protecció de les persones. La creació de fitxers de titularitat privada ha d'anar antecedida per la notificació a l'AEPD. El Registre General de Protecció de Dades procedeix a la inscripció del fitxer si la notificació s'ajusta als requisits exigibles. Aquesta pot ser concedida per silenci administratiu. La LOPD fa una regulació específica d'alguns fitxers de titularitat privada:

- Fitxers que contenen dades de solvència patrimonial. La cessió d'informació relativa a la solvència patrimonial té una excepció al consentiment de l'afectat que està motivada per raons d'interès públic representat en la protecció de l'interès públic.
- Fitxers amb finalitat de publicitat i prospecció comercial. Es regula especialment l'origen de les dades i el dret dels afectats a conèixer-lo. En relació amb aquestes dades pròpies del que es coneix com a *màrqueting relacional* és d'interès tenir en compte que la LSSI regula les comunicacions comercials per via electrònica (art.19-22). Finalment, cal assenyalar que la LOPD regula el cens promocional elaborat per l'Institut Nacional d'Estadística o òrgan equivalent de les comunitats autònomes amb una vigència anual que estarà format amb les dades de nom, cognoms i domicili que consten en el cens electoral.

#### **k) Com s'ha de garantir la seguretat de les dades?**

Sota aquest títol s'inclouen operacions tan diverses com els mecanismes de seguretat i secret de les dades fins a la consulta i accés a les dades i, si s'escau, la seva rectificació o cancel·lació. Els responsables dels fitxers tenen l'obligació de garantir la seguretat i guardar el secret professional de les dades a què tenen accés. Pel que fa als titulars de les dades, tenen dret a accedir de forma gratuïta a la informació sobre les seves dades de caràcter personal i el dret a rectificar i cancel·lar les dades d'un fitxer. També tenen dret d'empara i d'indemnització.

**Seguretat de les dades.** El responsable del fitxer i l'encarregat del tractament tenen el deure d'adoptar les mesures d'índole tècnica i organitzativa necessàries per a garantir la seguretat de les dades de caràcter personal i evitar-ne l'alteració, pèrdua, tractament o accés no autoritzat, segons l'estat de la tecnologia, la naturalesa de les dades i els riscos a què estiguin exposats. Per a garantir la seguretat no es registraran dades de caràcter personal en fitxers que no reuneixin les condicions determinades reglamentàriament. La finalitat de les mesures de seguretat és la de garantir la confidencialitat (permetre el coneixement de les dades només als usuaris autoritzats), integritat (impedir l'alteració de la informació) i disponibilitat de les dades (de manera que la informació sigui utilitzada pels usuaris autoritzats).

**Deure de secret.** El responsable del fitxer i els qui intervinguin en qualsevol fase del tractament de les dades de caràcter personal estan obligats al secret professional respecte de les dades i al deure de guardar-les fins i tot després de finalitzar les seves relacions amb el titular del fitxer automatitzat.

### l) Com es pot accedir a les dades?

**Accés a les dades.** Tot interessat pot sol·licitar i obtenir gratuïtament informació sobre les seves dades de caràcter personal sotmeses a tractament, l'origen i les comunicacions realitzades o que es prevegi fer. Aquest dret es pot exercir únicament a intervals no inferiors a dotze mesos.

Amb caràcter previ es pot exercir el dret de consulta que implica el dret a conèixer l'existència d'un determinat tractament de dades de caràcter personal demanant informació al Registre General de Protecció de Dades.

**Rectificació i cancel·lació.** Com a conseqüència de l'exercici dels drets de rectificació i cancel·lació que hem exposat anteriorment, el responsable del tractament té l'obligació de fer efectiu el dret de rectificació o cancel·lació en el termini de deu dies. Cancel·lar no és sinònim d'esborrar, sinó que implica bloquejar les dades conservant-les únicament perquè l'Administració o els tribunals puguin, si escau, determinar les responsabilitats nascudes del tractament. La regulació de l'exercici dels drets de rectificació i cancel·lació es troba en el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999. És interessant assenyalar que per a aquells casos en què l'exercici d'aquests drets hagi donat un resultat infructuós per l'oposició i reticències del responsable del fitxer o de l'encarregat del tractament, la LOPD preveu un procediment de tutela davant l'Agència Espanyola de Protecció de Dades. A més, si s'han causat danys o lesió en els béns o drets dels afectats tenen dret a ser indemnitzats.

### m) Què és la transferència internacional de dades?

En relació amb el moviment internacional de dades, cal tenir en compte que la Directiva 95/46 estableix el sistema de protecció de dades sobre la base del principi segons el qual les dades de caràcter personal constitueixen béns que s'integren dins del comerç. En conseqüència, les llibertats de tràfic de béns, persones i serveis que s'estableixen com a llibertats bàsiques per a la consecució de la Unió Europea s'apliquen de manera idèntica a les dades com a qualsevol altre bé.

Per tant, només hi ha una transferència internacional de dades quan el país de destinació és un estat no membre de la Unió Europea. En relació amb aquests països, la LOPD estableix que no es poden fer transferències internacionals de dades a països que no proporcionin nivells de protecció i seguretat equiparables als previstos en la mateixa norma, llevat que ho autoritzi l'Agència Espanyola de Protecció de Dades. La Directiva 95/46 estableix que la Comissió pot fer constar que un país tercer garanteix un nivell de protecció adequat.

#### **n) Què passa si s'infringeix la regulació de la protecció de dades personals?**

La LOPD estableix un règim de responsabilitat administrativa per a aquells casos en què s'infringeixi l'ordenament que implica la imposició d'una sanció. Aquest règim és diferent en funció que es tracti de fitxers de titularitat privada (art. 43.1) o de titularitat pública (art. 43.2). La potestat sancionadora correspon a l'Agència Espanyola de Protecció de Dades. La LOPD regula qui s'entenen com a responsables als efectes de la Llei i gradua les infraccions en lleus, greus o molt greus.

La LOPD també regula un règim de responsabilitat civil amb l'objectiu de reparar els danys causats a tercers. És aplicable a aquells casos en què el responsable del fitxer o l'encarregat del tractament incompleixin el que preveu la LOPD i causin un dany a l'afectat. És una naturalesa de caràcter objectiu. L'aplicació d'aquest règim de responsabilitat és aplicable a aquells supòsits en què s'hagi lesionat algun dret fonamental o llibertat pública.

En tenir finalitats diferents, poden concórrer o existir l'una sense l'altra.

## 2. Les dades personals a l'administració pública

### Lectura proposada

M. Fernández Salmerón. *Protección de datos personales y Administración pública electrónica*. Mòdul didàctic. UOC.

En relació amb els diferent usos dels mitjans electrònics a l'administració pública, es proposa la lectura dels següents treballs:

#### a) Difusió de la informació del sector públic

Aquests treballs aborden la tensió entre la transparència i la difusió d'informació del sector públic i la protecció de les dades personals en poder de les administracions públiques:

Fernández Salmerón, M.; Valero Torrijos, J. (2008). "La difusión de información administrativa en Internet y la protección de los datos personales: análisis jurídico de un proceso de armonización". A: A. Troncoso Reigada (ed.). *Transparencia administrativa y protección de datos personales. V Encuentro entre Agencias Autonómicas de Protección de Datos*. Madrid: Thomson-Civitas. <<http://goo.gl/4gQoHH>>

Guichot Reina, E. (2008). "Acceso a la información y protección de datos. Estado de la cuestión". A: A. Troncoso Reigada (ed.). *Transparencia administrativa y protección de datos personales. V Encuentro entre Agencias Autonómicas de Protección de Datos*. Madrid: Thomson-Civitas. <<http://goo.gl/HHO77q>>

Guichot Reina, E. (2007). "Acceso a la información en poder de la Administración y protección de datos personales". *Revista de Administración Pública* (núm. 173). <<http://www.cepc.gob.es/publicaciones/revistas/revistaselectronicas?IDR=1&IDN=624&IDA=26523>>

Guichot Reina, E. (2007). "Derecho a la privacidad, transparencia y eficacia administrativa: un difícil y necesario equilibrio". *Revista Catalana de Dret Públic* (núm. 35). <<http://goo.gl/IWoR8S>>

#### b) Tramitació del procediment administratiu

Aquests treballs analitzen l'impacte de la protecció de les dades personals en la tramitació del procediment administratiu a través de mitjans electrònics i l'impacte de la interoperabilitat. També cal tenir en compte la regulació de la signatura electrònica i el seu ús en les relacions entre les administracions públiques i els ciutadans.

**Troncoso Reigada, A.** (2008). “La administración electrónica y la protección de datos personales”. *Revista Jurídica de Castilla y León*. <<http://www.navarra.es/NR/rdonlyres/E6188543-88F9-476F-8581-406069D3C0E7/188896/32AdministracionelectronicayprotecciondedatosTronc.pdf>>

**Rallo Lombarte, A.** (2010). “La Administración electrónica y el derecho a la protección de datos personales”. A: C. de la Hera Pascual (ed.). *Administración electrónica: estudios, buenas prácticas y experiencias en el ámbito local*. Madrid: Fundación Democracia y Gobierno Local.

<[http://repositorio.gobiernolocal.es/xmlui/bitstream/handle/10873/967/claves12\\_06\\_rallo.pdf?sequence=1](http://repositorio.gobiernolocal.es/xmlui/bitstream/handle/10873/967/claves12_06_rallo.pdf?sequence=1)>



## Bibliografía

**Fernández Salmerón, M.; Valero Torrijos, J.** (2008). "La difusión de información administrativa en Internet y la protección de los datos personales: análisis jurídico de un proceso de armonización". A: A. Troncoso Reigada (ed.). *Transparencia administrativa y protección de datos personales. V Encuentro entre Agencias Autonómicas de Protección de Datos*. Madrid: Thomson-Civitas.

**Guichot Reina, E.** (2007). "Acceso a la información en poder de la Administración y protección de datos personales". *Revista de Administración Pública* (núm. 173).

**Guichot Reina, E.** (2007). "Derecho a la privacidad, transparencia y eficacia administrativa: un difícil y necesario equilibrio". *Revista Catalana de Dret Públic* (núm. 35).

**Guichot Reina, E.** (2008). "Acceso a la información y protección de datos. Estado de la cuestión". A: A. Troncoso Reigada (ed.). *Transparencia administrativa y protección de datos personales. V Encuentro entre Agencias Autonómicas de Protección de Datos*. Madrid: Thomson-Civitas.

**Rallo Lombarte, A.** (2010). "La Administración electrónica y el derecho a la protección de datos personales". A: C. de la Hera Pascual (ed.). *Administración electrónica: estudios, buenas prácticas y experiencias en el ámbito local*. Madrid: Fundación Democracia y Gobierno Local.

**Troncoso Reigada, A.** (2008). "La administración electrónica y la protección de datos personales". *Revista Jurídica de Castilla y León*.

