La protecció de dades personals a l'administració pública

PID_00272671

Agustí Cerrillo Martínez

Temps mínim de dedicació recomanat: 3 hores

Universitat Oberta de Catalunya

Agustí Cerrillo Martínez

Catedrático de Derecho Administrativo en la Universitat Oberta de Catalunya (UOC).

La revisió d'aquest recurs d'aprenentatge UOC ha estat coordinada pel professor: Agustí Cerrillo i Martínez (2020)

Tercera edició: febrer 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Realització editorial: FUOC

Índex

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, quina 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

J. J. Fernández Rodríguez (2018). "Decálogo sobre a nova normativa de protección de datos". *Administración & cidadanía: Revista da Escola Galega de Administración Pública* (vol. 2, núm. 13, pàg. 61-78). <https://egap.xunta.gal/Documentos/Publicacions/[1563537639]Revista_AC_13_2_web.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-hi 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 (article 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'article18.4 CE estableix que la "llei limitarà l'ús de la informàtica per garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets".

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·limitats 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".[1]

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

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".[2]

(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'article18.4 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 intromisions 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".[3]

[(3)]Vegeu també la STC 143/1994, de 9 de maig, FJ 7.

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.

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) Quin impacte té la protecció de dades en la transparència pública?

Lectures proposades

A. Cerrillo i Martínez (2017). "El difícil equilibrio entre transparencia pública y la protección de datos personales". *Cuadernos de Derecho Local* (núm. 45).

E. Guichot Reina (2017). "Las relaciones entre publicidad y privacidad en la normativa sobre transparencia y acceso a la información". *Cuadernos de Derecho Local* (núm. 44, pàg. 12-47).

e) 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, es va aprovar 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 va constatar que la Directiva 95/46 havia assolit l'objectiu d'atorgar una protecció suficient

(4)Vegeu l'informe a: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52003DC0265.

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.[4]

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.

El 2016 es va aprovar el Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril del 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46 CE (Reglament general de protecció de dades) que té efecte directe sense necessitat de ser transposat.

L'RGPD introdueix importants novetats en matèria de protecció de dades i té una incidència especial en les administracions públiques.

Vegeu, en síntesi, el document:

Agència Espanyola de Protecció de Dades (2017). *El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones Públicas*. <https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AAPP.pdf>

La legislació europea ha estat traslladada a l'ordenament jurídic espanyol mitjançant la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD) i, en determinats aspectes, per la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació (LSSI). La LOPDGDD va derogar la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD).

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. L'Agència de Protecció de Dades de la Comunitat de Madrid va ser suprimida l'1 de gener de 2013 per la Llei 8/2012, de 28 de desembre, de mesures fiscals i administratives 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. Sobre això, l'RGPD reconeix que els codis de conducta estan destinats a contribuir a la correcta aplicació del Reglament per mitjà de l'especificació de la seva aplicació en relació amb aspectes com ara el tractament lleial i transparent, els interessos legítims perseguits pels responsables del tractament en contextos específics, la recollida de dades personals, la informació proporcionada al públic i als interessats, o l'exercici dels drets dels interessats. El codi de conducta ha de contenir mecanismes que permetin efectuar el control obligatori del compliment de les seves disposicions pels responsables o encarregats del tractament que es comprometin a aplicar-lo. El codi serà registrat i publicat per l'autoritat de control corresponent.

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

L'Agència Espanyola de Protecció de Dades és una autoritat administrativa independent d'àmbit estatal 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 reclamacions dels afectats.

- Promoure la sensibilització del públic i la seva comprensió dels riscos, normes, garanties i drets en relació amb el tractament i dels responsables i encarregats del tractament sobre les obligacions que els afecten.

- Cooperar, en particular, compartint informació amb altres autoritats de control i prestar assistència mútua a fi de garantir la coherència en l'aplicació i execució de l'RGPD.

Per aconseguir aquests fins, el mateix reglament reconeix tot un seguit de potestats com són les d'ordenar al responsable i a l'encarregat del tractament que facilitin qualsevol informació, dur a terme investigacions en forma d'auditories de protecció de dades, dur a terme una revisió de les certificacions expedides o notificar al responsable o l'encarregat del tractament les presumptes infraccions del Reglament.

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 jurisdiccionals 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 (article 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 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. En l'actualitat, l'Autoritat Catalana de Protecció de Dades, creada per la Llei 32/2010, d'1 d'octubre, disposa que té per objecte garantir, en l'àmbit de les competències de la Generalitat, els drets a la protecció de dades personals i d'accés a la informació que hi està vinculada.

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 pú-

bliques 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.

g) Què és una dada personal?

La primera qüestió que s'ha de delimitar és la relativa a què s'entén per *dada*. D'acord amb l'RGPD, una dada personal és qualsevol informació sobre una persona física identificada o identificable (l'interessat). S'ha de considerar persona física identificable qualsevol persona la identitat de la qual es pot determinar, directament o indirectament, mitjançant un identificador, com per exemple un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona.

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.

L'ús de les noves tecnologies ha plantejat en el passat si determinada informació havia de ser considerada com a dada de caràcter personal. En particular, la pregunta s'havia formulat respecte a si l'adreça de correu electrònic i l'adreça d'IP eren 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".

h) Quins són els principis relatius al tractament?

Els principis relatius al tractament són aquelles regles que regulen com s'ha de dur a terme el tractament de les dades personals amb la finalitat de garantir-ne la protecció.

D'aquesta manera, les dades personals han de ser necessàriament tractades d'acord amb els principis previstos en l'RGPD. La vulneració dels principis previstos en l'RGPD es tipifica en la normativa vigent com a infracció molt greu.[5]

(5) Articles 83 RGPD i 72 LOPDGDD.

L'RGPD ha dut a terme una actualització dels diferents principis als quals farem referència a continuació. No obstant això, en termes generals, la regulació dels principis del tractament té un caràcter continuista respecte a la regulació anterior, tot i que s'han incorporat nous principis com el de la responsabilitat proactiva.

Principis de licitud, lleialtat i transparència. Les dades personals han de ser tractades de manera lícita, lleial i transparent en relació amb l'interessat.[6]

(6) Article 5.1.a RGPD.

Perquè el tractament sigui lícit cal que es doni alguna de les condicions previstes en l'RGPD.[7]

(7) Article 6.1 RGPD.

La principal condició perquè el tractament sigui lícit és que l'interessat hagi donat el seu consentiment per al tractament de les seves dades personals per a un o diversos fins específics. El consentiment ha de ser lliure, específic, informat i inequívoc pel qual accepta, sigui mitjançant una declaració o una clara acció afirmativa, el tractament de les dades personals que el concerneixen.[8]

(8) Article 4.11 RGPD.

Perquè el consentiment es pugui manifestar adequadament, cal facilitar als interessats informació sobre el tractament de manera concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill.[9] L'RGPD preveu que la informació que s'hagi de facilitar a l'interessat serà diferent quan les dades personals s'obtinguin de l'interessat (article 13.1) respecte a quan les dades personals no s'hagin obtingut de l'interessat (article 14.1 i 2). En tots dos casos, el responsable del tractament pot facilitar a l'afectat la informació bàsica indicant-li l'adreça de correu electrònic o el mitjà a la seva disposició per a poder accedir a la informació restant.[10]

(9) Article 12 RGPD.

(10) Article 11 LOPDGDD.

A més dels supòsits en què l'interessat ha donat el seu consentiment, els tractaments de les dades personals poden ser lícits si calen per a l'execució d'un contracte en el qual l'interessat sigui part o per a l'aplicació a petició d'aquest de mesures precontractuals, per al compliment d'una obligació legal aplicable al responsable del tractament, per a protegir interessos vitals de l'interessat o d'una altra persona física, per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament,

(11) Article 6.1 RGPD.

o per a la satisfacció d'interessos legítims perseguits pel responsable del tractament o per un tercer, sempre que sobre aquests interessos no prevalguin els interessos o els drets i llibertats fonamentals de l'interessat que requereixin la protecció de les dades personals.[11]

Lectura proposada

A. Cerrillo i Martínez (2019, juliol). "Las características del consentimiento del interesado y su incidencia en el tratamiento de datos en las administraciones públicas". *El Consultor de los Ayuntamientos*, III.

Principi de limitació de la finalitat. Les dades personals han de ser recollides amb finalitats determinades, explícites i legítimes, i no seran tractades ulteriorment de manera incompatible amb aquestes finalitats.[12]

(12)Article 5.1.b RGPD.

Aquest precepte també disposa que el tractament posterior de les dades personals amb finalitats d'arxiu en interès públic, amb finalitats de recerca científica i històrica o amb finalitats estadístiques no es considera incompatible amb les finalitats inicials.[13]

(13)Vegeu al respecte el que disposa l'article 26 LOPDGDD.

Amb relació a la limitació de la finalitat, l'LRJSP[14] preveu que si bé les administracions públiques han de facilitar a altres administracions públiques l'accés a les dades relatives als interessats que estiguin en el seu poder, aquestes no poden dur a terme un tractament d'aquestes dades amb finalitats incompatibles amb la finalitat per la qual es van recollir inicialment les dades personals.

(14)Article 155 apartats 2 i 3 LRJSP modificats pel Reial decret llei 14/2019 de 31 d'octubre.

En particular, s'estableix que quan l'Administració pública cessionària de les dades pretengui el seu tractament ulterior per a una finalitat que estimi compatible amb la finalitat inicial, ho ha de comunicar prèviament a l'Administració pública cedent perquè aquesta pugui comprovar aquesta compatibilitat. Aquesta s'hi pot oposar de manera motivada en el termini de deu dies.

Fins que l'Administració pública cedent no comuniqui la seva decisió, l'Administració pública cessionària no podrà utilitzar les dades per a la nova finalitat pretesa, excepte que així estigui previst en una norma amb rang de llei.

Principi de minimització de dades. Les dades personals han de ser adequades, pertinents i limitades a allò que calgui en relació amb les finalitats per a les quals són tractades.[15]

(15)Article 5.1.c RGPD.

D'aquesta manera, cal assegurar que únicament es recullen les dades personals necessàries per a aconseguir la finalitat prevista.

Principi d'exactitud. Les dades personals han de ser exactes i, si cal, actualitzades.[16]

(16)Article 5.1.d RGPD.

Per a això, cal adoptar totes les mesures raonables perquè se suprimeixin o rectifiquin sense dilació les dades personals que siguin inexactes respecte als fins per als quals es tracten.

Principi de seguretat. Les dades personals han de ser tractades de tal manera que es garanteixi de manera adequada la seva seguretat per a evitar, entre d'altres, el tractament no autoritzat o il·lícit, la pèrdua, destrucció o dany accidental.

D'aquesta manera es persegueix garantir la integritat i la confidencialitat de les dades.

i) Quins són els drets de les persones respecte a les dades personals?

Per a garantir el compliment d'aquests principis, l'RGPD reconeix diferents drets dels interessats. L'RGPD ha reforçat els drets dels interessats en matèria de protecció de dades. També ha ampliat els drets entre els quals podem destacar el dret a l'oblit que, amb anterioritat a la seva regulació en l'RGPD, va ser objecte d'atenció pel Tribunal de Justícia de la Unió Europea.[17]

(17)Sentència del TJUE, de 13 de maig de 2014, assumpte C - 131/12 Google Spain, SL i Google Inc. / Agència Espanyola de Protecció de Dades, Mario Costeja González.

(18)Títol X LOPDGDD.

Al costat dels drets reconeguts en l'RGPD, la LOPDGDD reconeix altres drets dels ciutadans a internet, com ara el dret a l'educació digital, el dret a la intimitat i ús de dispositius digitals en l'àmbit laboral, el dret a la desconnexió digital en l'àmbit laboral, el dret a la intimitat enfront de l'ús de dispositius de videovigilància i de gravació de sons al lloc de treball, el dret a la intimitat davant la utilització de sistemes de geolocalització en l'àmbit laboral o el dret a l'oblit a cerques d'internet.[18]

En relació amb els diferents drets reconeguts, cal tenir present els aspectes següents de caràcter general.

En primer lloc, que el responsable del tractament està obligat a indicar a l'interessat els mitjans a la seva disposició per a exercir els drets. Aquests mitjans han de ser fàcilment accessibles.[19]

(19)Article 12 LOPDGDD.

En segon lloc, que els drets reconeguts en l'RGPD poden ser limitats quan amb la restricció es respectin els drets i llibertats fonamentals i sigui una mesura necessària i proporcionada per a salvaguardar, entre d'altres, la seguretat de l'Estat, la defensa, la seguretat pública, la prevenció, la investigació, la detecció o l'enjudiciament d'infraccions penals o l'execució de sancions penals, la protecció de la independència judicial, la supervisió, la inspecció, la reglamentació vinculada amb l'exercici de l'autoritat pública o la protecció de l'interessat o dels drets i llibertats dels altres.[20]

(20)Article 23 RGPD.

En tercer lloc, que en el cas que no es respectin els drets reconeguts en l'RGPD, l'interessat pot presentar una reclamació davant l'Agència Espanyola de Protecció de Dades o l'agència autonòmica de protecció de dades competent, la qual ha de resoldre sobre això.[21] Així mateix, l'impediment o l'obstaculització de l'exercici dels interessats està tipificat com a infracció.[22]

(21)Considerant 141 RGPD, i també, entre d'altres, els articles 12.4, 13.2, 14.2, 15.1 RGPD.

(22)Articles 83 RGPD i 72.1.ky 74.cyd LOPDGDD.

Dret d'informació. La transparència en el tractament de les dades personals es concreta en el dret a la informació dels interessats.

Com ja hem avançat anteriorment, els responsables del tractament han d'informar l'interessat de diversos aspectes que variaran en funció de si les dades de l'interessat han estat recollides o no.

No obstant això, l'RGPD disposa d'algunes excepcions a aquest dret com, per exemple, quan la informació ja estigui a disposició de l'interessat.[23]

(23)Article 14.5 RGPD.

En termes generals, la informació s'ha de posar a disposició dels interessats en el moment en què se li sol·licitin les seves dades o, quan les dades no s'obtinguin del propi interessat, en el termini d'un mes.[24]

(24)Article 14.3 RGPD.

Dret d'accés. L'interessat té dret a saber si s'estan tractant o no les seves dades personals.[25]

(25)Article 15.1 RGPD.

L'interessat també té dret a accedir a aquestes dades i a obtenir la informació relativa a diferents aspectes com ara els fins del tractament, les categories de dades personals de què es tracti, els destinataris o les categories de destinataris als quals es van comunicar o seran comunicades les dades personals, el termini previst de conservació de les dades personals o, si no és possible, els criteris utilitzats per a determinar aquest termini, l'existència del dret a sol·licitar del responsable la rectificació o supressió de dades personals o la limitació del tractament de dades personals relatives a l'interessat, o oposar-se a aquest trac-

tament, el dret a presentar una reclamació davant d'una autoritat de control o la informació disponible sobre el seu origen quan les dades personals no s'hagin obtingut de l'interessat i l'existència de decisions automatitzades.

Quan així ho sol·liciti l'interessat, el responsable del tractament li facilitarà una còpia de les dades personals objecte de tractament sense que això pugui afectar negativament els drets i llibertats de tercers. La LOPDGDD disposa que el dret s'entendrà atorgat si el responsable del tractament facilita a l'interessat un sistema d'accés remot, directe i segur a les seves dades personals.[26]

(26)Article 13 RGPD.

Dret de rectificació. L'interessat té dret a obtenir sense dilació indeguda la rectificació de les dades personals inexactes que li concerneixin.[27]

(27)Article 16 RGPD.

L'interessat té dret que es completin les dades personals que siguin incomplertes.

A aquests efectes, l'interessat ha d'indicar de manera clara i detallada a quines dades es refereix i la correcció que s'hagi de fer i, quan calgui, acompanyar la sol·licitud de la documentació que justifiqui la rectificació.[28]

(28)Article 14 LOPDGDD.

Dret de supressió. L'interessat té dret a obtenir sense dilació indeguda la supressió de les dades personals que li concerneixin.[29]

(29)Article 17 RGPD.

El responsable del tractament estarà obligat a suprimir les dades personals de l'interessat quan aquestes ja no calguin en relació amb les finalitats per les quals van ser recollides o tractades d'una altra manera, l'interessat retiri el consentiment en què es basa el tractament, l'interessat s'oposi al tractament i no prevalguin altres motius legítims per al tractament, les dades personals hagin estat tractades il·lícitament, les dades personals s'hagin de suprimir per al compliment d'una obligació legal o s'hagin obtingut en relació amb l'oferta de serveis de la societat de la informació.

El dret de supressió pot ser limitat quan calgui el tractament per a exercir el dret a la llibertat d'expressió i informació; per al compliment d'una obligació legal o per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable; per raons d'interès públic en l'àmbit de la salut pública; amb fins d'arxiu en interès públic, fins d'investigació científica o històrica, o finalitats estadístiques o per a la formulació, l'exercici o la defensa de reclamacions.

Dret a la limitació del tractament. L'interessat té dret a obtenir del responsable del tractament la limitació del tractament de les dades.

La limitació del tractament es podrà obtenir quan l'interessat hagi impugnat l'exactitud de les dades personals o el tractament sigui il·lícit i l'interessat s'oposi a la supressió de les dades personals i sol·liciti en el seu lloc la limitació del seu ús; o el responsable ja no necessiti les dades personals per a les finalitats del tractament, però l'interessat les necessiti per a la formulació, l'exercici o la defensa de reclamacions; o l'interessat s'hagi oposat al tractament mentre es verifica si els motius legítims del responsable prevalen sobre els de l'interessat.[30]

(30)Article 18 RGPD.

Quan s'hagi limitat el tractament de les dades personals, les dades només poden ser objecte de tractament, a excepció de la seva conservació, amb el consentiment de l'interessat o per a la formulació, l'exercici o la defensa de reclamacions, o amb vista a la protecció dels drets d'una altra persona física o jurídica o per raons d'interès públic important.

Dret d'oposició. L'interessat té dret a oposar-se en qualsevol moment, per motius relacionats amb la seva situació particular, al fet que les dades personals que li concerneixen siguin objecte d'un tractament.[31]

(31)Article 21 RGPD.

En aquest cas, el responsable del tractament ha de deixar de tractar les dades personals, llevat que acrediti motius legítims imperiosos per al tractament que prevalguin sobre els interessos, els drets i les llibertats de l'interessat, o per a la formulació, l'exercici o la defensa de reclamacions.

Una manifestació concreta d'aquest dret la trobem en el dret a no ser objecte d'una decisió basada únicament en el tractament automatitzat de les dades personals que produeixi efectes jurídics en aquest o l'afecti significativament de manera similar.[32]

(32)Article 22 RGPD.

j) Els responsables i els encarregats del tractament

Les administracions públiques, quan siguin responsables del tractament, han d'aplicar mesures tècniques i organitzatives apropiades per tal de garantir i poder demostrar que el tractament segueix l'RGPD.[33] Aquestes mesures han de ser dissenyades d'acord amb la naturalesa, l'àmbit, el context i les finalitats del tractament, així com dels riscos de diversa probabilitat i gravetat per als drets i llibertats de les persones físiques

(33)Article 24 RGPD.

Entre aquestes mesures hi ha la de triar un encarregat de tractament als quals l'RGPD atribueix obligacions específiques als encarregats. L'encarregat ha d'oferir prou garanties per aplicar mesures tècniques i organitzatives apropiades, d'acord amb les instruccions del responsable, de manera que el tractament sigui conforme amb els requisits de l'RGPD i garanteixi la protecció dels drets de l'interessat.[34]

(34)Article 28 RGPD.

k) El delegat de protecció de dades en una Administració pública

Quan el tractament el porti a terme una Administració pública, el responsable i l'encarregat del tractament han de designar un delegat de protecció de dades.[35] Es pot designar un únic delegat de protecció de dades per a diverses administracions públiques o organismes, tenint en compte la seva estructura organitzativa i grandària.

(35)Article 37 RGPD. Vegeu Agència Espanyola de Protecció de Dades (2017). *El Delegado de Protección de Datos en las Administraciones Públicas*. Accés a: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Funciones_DPD_en_AAPP.pdf

El delegat de protecció de dades ha de ser designat tenint en compte les seves qualitats professionals i, en particular, els seus coneixements especialitzats de la regulació i la pràctica en matèria de protecció de dades, així com la seva capacitat per a exercir les funcions previstes a l'RGPD.

El delegat de protecció de dades pot formar part de la plantilla del responsable o de l'encarregat del tractament o exercir les seves funcions en el marc d'un contracte de serveis. A més, el delegat de protecció de dades podrà exercir altres funcions i comeses. El responsable o encarregat del tractament ha de garantir que aquestes funcions i comeses no donen lloc a un conflicte d'interessos.

El delegat de protecció de dades té diverses funcions, entre les quals destaquen les següents:[36]

(36)Article 39 RGPD.

a) Informar i assessorar el responsable o l'encarregat del tractament i els empleats que s'ocupin del tractament de les obligacions de què s'han de fer càrrec en virtut de l'RGPD i d'altres disposicions de protecció de dades de la Unió o dels estats membres.

b) Supervisar el compliment del que disposa l'RGPD, d'altres disposicions de protecció de dades de la Unió o dels estats membres i de les polítiques del responsable o de l'encarregat del tractament en matèria de protecció de dades personals, inclosa l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament i les auditories corresponents.

c) Oferir l'assessorament que se li demani sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar la seva aplicació de conformitat amb l'article 35.

d) Cooperar amb l'autoritat de control.

e) Actuar com a punt de contacte de l'autoritat de control per qüestions relatives al tractament, inclosa la consulta prèvia a què es refereix l'article 36, i realitzar consultes, si s'escau, sobre qualsevol altre assumpte.

El responsable i l'encarregat del tractament han de garantir que el delegat de protecció de dades participi adequadament i en temps oportú en totes les qüestions relatives a la protecció de dades personals i que no rebi cap instrucció

pel que fa a l'exercici d'aquestes funcions. El delegat de protecció de dades no pot ser destituït ni sancionat pel responsable o l'encarregat per exercir les seves funcions.

l) Els codis de conducta, els mecanismes de certificació i les normes corporatives vinculants (BCR)

L'RGPD preveu que els responsables de tractament poden adoptar diferents instruments per acreditar el compliment de les obligacions previstes.

L'adhesió a un codi de conducta o a un mecanisme de certificació pot servir d'element per demostrar el compliment de les obligacions per part del responsable del tractament.[37]

(37)Article 24 RGPD.

Les administracions públiques poden adoptar codis de conducta, així com promoure l'elaboració de codis de conducta destinats a contribuir a la correcta aplicació de l'RGPD.[38] Els codis de conducta han de recollir diferents aspectes relatius a l'aplicació de l'RGPD en relació amb l'Administració pública que l'adopta, com la recollida de dades personals, la informació que es facilita als interessats, els drets dels interessats, les responsabilitats del responsable i de l'encarregat del tractament, les mesures de seguretat adoptades o els mecanismes de resolució de conflictes i de control del compliment del codi.[39]

(38)Article 40 RGPD.

(39)Article 40 RGPD.

Les administracions públiques també poden adoptar amb caràcter voluntari certificacions, de segells i marques de protecció de dades, per demostrar el compliment del que disposa l'RGPD en les operacions de tractament dels responsables i els encarregats que portin a terme.[40] Les administracions públiques, al costat de les autoritats de control, han de promoure la creació d'aquests mecanismes de certificació en matèria de protecció de dades.

(40)Article 42 RGPD.

Finament, les administracions públiques poden adoptar normes corporatives vinculants (BCR) com a garantia per poder fer transferències internacionals sense la necessitat d'obtenir una autorització específica quan la Comissió no hagi decidit que el tercer país, un territori o un o diversos sectors específics d'aquest tercer país, o l'organització internacional de què es tracti, garanteixen un nivell de protecció adequat. Les normes corporatives vinculants seran aprovades per l'autoritat de control.[41]

(41)Article 47 RGPD.

Quan hi hagi autorització per part de l'autoritat de control competent, les administracions públiques poden adoptar les garanties mitjançant disposicions que s'incorporin a acords administratius entre les autoritats o organismes públics que incloguin drets efectius i exigibles per als interessats.

m) Què passa si s'infringeix la regulació de la protecció de dades personals?

La LOPD establia un règim específic per a les infraccions comeses en fitxers de titularitat pública o en relació amb els tractaments els responsables ho eren de fitxers d'aquesta naturalesa. En aquests casos, es disposava que l'òrgan sancionador dictaria una resolució per a establir les mesures que procedís adoptar perquè cessessin o es corregissin els efectes de la infracció. Així mateix, es preveia la possibilitat que l'òrgan sancionador també pogués proposar la iniciació d'actuacions disciplinàries. No obstant això, no es preveia la possibilitat d'imposar les sancions de multa previstes aplicables per als fitxers de titularitat privada i els tractaments realitzats per entitats privades.

L'RGPD va obrir la possibilitat de canviar aquesta la situació, ja que va preveure que més enllà dels poders correctius de les autoritats de control, cada Estat membre pot establir normes sobre si es pot, i en quina mesura, imposar multes administratives a autoritats i organismes públics establerts en l'esmentat Estat membre.

Aquesta possibilitat ha estat pràcticament tancada per la LOPDGDD.

Aquesta norma disposa d'un règim sancionador aplicable a determinades categories de responsables o encarregats del tractament entre les quals hi ha els següents:

- Els òrgans constitucionals o amb rellevància constitucional i les institucions de les comunitats autònomes anàlogues als mateixos.
- Els òrgans jurisdiccionals.
- L'Administració General de l'Estat, les administracions de les comunitats autònomes i les entitats que integren l'Administració local.
- Els organismes públics i entitats de dret públic vinculades o dependents de les administracions públiques.
- Les autoritats administratives independents.
- El Banc d'Espanya.
- Les corporacions de dret públic quan les finalitats del tractament es relacionin amb l'exercici de potestats de dret públic.
- Les fundacions del sector públic.
- Les universitats públiques.
- Els consorcis.

- Els grups parlamentaris de les Corts Generals i les assemblees legislatives autonòmiques, i també els grups polítics de les corporacions locals.

Quan un responsable o encarregat inclòs en aquestes categories cometi una infracció, l'autoritat de protecció de dades que resulti competent dictarà resolució sancionant-lo amb apercebiment. Així mateix, es concretaran les mesures que s'han d'adoptar perquè cessi la conducta o es corregeixin els efectes de la infracció que s'hagi comès. A més, si les infraccions són imputables a autoritats i directius i s'acredita l'existència d'informes tècnics o recomanacions per al tractament que no hagin estat degudament atesos, en la resolució en la qual s'imposi la sanció s'inclourà una amonestació amb denominació del càrrec responsable i s'ordenarà la publicació al Butlletí Oficial de l'Estat o autonòmic que correspongui.

La LOPDGDD també disposa que la resolució es notificarà al responsable o encarregat del tractament, a l'òrgan del qual depengui jeràrquicament i als afectats que tinguin la condició d'interessats. A més, les resolucions es publicaran a la pàgina web de l'Agència Espanyola de Protecció de Dades quan aquesta sigui l'autoritat competent, amb expressa indicació de la identitat del responsable o encarregat del tractament que hagués comès la infracció.

Així mateix, es preveu que l'autoritat de protecció de dades proposi la iniciació d'actuacions disciplinàries quan hi hagi indicis suficients d'acord amb el que preveu la legislació sobre règim disciplinari o sancionador que sigui aplicable. Les resolucions que recaiguin s'hauran de comunicar a l'autoritat de protecció de dades.

Finalment, la LOPDGDD disposa que s'han de comunicar al Defensor del Poble o, si s'escau, a les institucions anàlogues de les comunitats autònomes les actuacions realitzades i les resolucions dictades.

Bibliografia

Agencia Española de Protección de Datos (2018). *Protección de datos y administración local*. Madrid: Agencia Española de Protección de Datos.

Grupo de trabajo para la implantación del nuevo Reglamento General de Protección de Datos (RGPD) en las Administraciones Locales-Federación Española de Municipios y Provincias (2018). *Guía para la adaptación del Reglamento General de Protección de Datos de las Administraciones Locales*. Madrid: Federación Española de Municipios y Provincias.

Jiménez Asensio, R. (2019). "El nuevo marco normativo de la protección de datos personales: su aplicación a las entidades locales".*Anuario Aragonés del Gobierno Local 2018* (núm. 10, pàg. 321-365).

Jiménez Asensio, R.; Moro, A. (2018). *Manual-guía sobre impactos del Reglamento (UE) de protección de datos en los entes locales*. Barcelona: Federació de Municipis de Catalunya-Associació Catalana de Municipis.