Introducció a la protecció de dades de caràcter personal

PID_00261931

Mònica Vilasau Solana
Miquel Peguera

Temps mínim de dedicació recomanat: 4 hores

Universitat Oberta de Catalunya

Mònica Vilasau Solana

Professora de Dret Civil als Estudis de Dret i Ciència Política de la Universitat Oberta de Catalunya. Doctora en Dret per la Universitat de Barcelona. Directora del Postgrau en Protecció de Dades de la UOC.

Miquel Peguera

Professor agregat de Dret Mercantil a la Universitat Oberta de Catalunya. Doctor en Dret per la Universitat de Barcelona. Affiliate Scholar, Center for Internet & Society (Stanford).

Primera edició: febrer 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Disseny: Manel Andreu
Realització editorial: Oberta UOC Publishing, SL

Índex

Introducció

Les dades de caràcter personal constitueixen la matèria primera de la societat de la informació; alguns autors les qualifiquen com el petroli de l'economia digital, de manera que difícilment els serveis públics, la societat del benestar o les empreses poden funcionar sense ells.

En contra del que podria semblar, aquestes dades (qualsevol informació relativa a una persona identificada o identificable) no es poden fer servir sense més ni més, sinó que s'han de respectar unes regles que disposen quan i com tractar-les. La preocupació per establir un marc regulador de la utilització de la informació personal va sorgir amb l'adveniment dels primers ordinadors. En el marc internacional, les primeres iniciatives van sorgir en el si del Consell d'Europa. La Resolució del 1968 va establir les bases d'uns principis que van regular el tractament de la informació personal. A partir d'aquí es van anar succeint les normes, tant a escala internacional com de la UE, nacional i autonòmica. En el context europeu, la principal norma que regula el tractament de la informació personal és el Reglament General de Protecció de Dades (RGPD), Reglament (UE) 2016/679 del Parlament Europeu i del Consell, del 27 d'abril del 2016.

Aquesta norma estableix les regles que qualsevol tractament de la informació personal ha de complir. No obstant això hi ha més disposicions que regulen aspectes concrets o matèries específiques de tractament de la informació personal. Per exemple, la Directiva 2016/680, relativa al tractament per a finalitats de prevenció, investigació, detecció o enjudiciament d'infraccions penals.

A nivell estatal, la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de dades personals i garantia dels drets digitals (LOPDGDD), substitueix la Llei Orgànica de Protecció de dades de caràcter personal (LOPD) de 1999, adapta el dret espanyol al marc establert pel RGPD i desenvolupa alguns aspectes d'aquest Reglament que es deixen a les legislacions nacionals. A més d'aquesta Llei, hi ha un ventall de disposicions que de manera directa o indirecta afecten el tractament de la informació personal. Entre altres cal destacar: la Llei 9/2014, de 9 de maig, general de telecomunicacions, o la Llei 34/2002, d'11 de juliol, de Serveis de la Societat de la informació i de comerç electrònic (LSSI).

Així mateix, cal destacar normes autonòmiques com ara la Llei 32/2010 d'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades; 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, o bé la Llei 1/2014, de 24 de juny, de Transparència Pública d'Andalusia.

Aquest mòdul vol ser una introducció a les regles bàsiques que permeten tractar la informació personal, que després es concretaran en sectors específics: comerç electrònic, banca, salut, o relacions laborals. Es tracta, en definitiva, d'adquirir uns coneixements bàsics, la cartografia que permetrà posteriorment navegar en les normes específiques que hi ha a diferents nivells. Aquests coneixements s'han d'aplicar a realitats que van sorgint i que de vegades no tenen encara una regulació específica o és molt incipient. Entre altres supòsits, l'internet de les coses, les xarxes socials, la computació en el núvol, les dades massives o el creixent recurs a la robòtica.

En els apartats següents s'analitza en primer lloc què és una dada personal, els principis que han de regir el tractament de la informació personal, l'àmbit subjectiu (qui tracta les dades i qui és el subjecte afectat) i els drets i deures de cadascun d'aquests protagonistes. A més, es dedica un epígraf específic al dret a l'oblit, en la mesura que en el moment d'adoptar-se el RGPD s'hi va posar molt d'èmfasi.

El dret a l'oblit constitueix una manifestació concreta dels drets de supressió o d'oposició al tractament. Una aplicació específica d'aquest dret es refereix a la possibilitat d'exigir als cercadors d'internet que eliminin determinats resultats quan les cerques es duen a terme a partir del nom d'una persona. El TJUE va afirmar aquest dret en la seva famosa sentència del cas Google Spain, del 13 de maig del 2014. Des de llavors, s'ha anat aplicant pels cercadors i l'han reconegut les autoritats de protecció de dades i els tribunals. Amb la seva aplicació pràctica s'han anat consolidant alguns criteris d'interpretació, però queden encara aspectes discutits en què la jurisprudència no és homogènia.

Objectius

1. Saber quan es pot aplicar el RGPD.

2. Aprendre i identificar els principis de protecció de dades.

3. Entendre el concepte de bases legals que permeten un tractament de dades.

4. Identificar els subjectes que intervenen en un tractament i conèixer-ne els drets i obligacions.

5. Conèixer els mecanismes de *soft law*.

6. Aprendre quins són els drets de l'afectat i les seves limitacions.

7. Saber el règim jurídic bàsic de les transferències internacionals de dades i el règim de responsabilitats i sancions.

1. El Reglament General de Protecció de Dades

Mònica Vilasau Solana

1.1. Quan és aplicable el RGPD?

1.1.1. En funció de l'àmbit material

L'article 1.1 RGPD té per objecte establir «les normes relatives a la protecció de les persones físiques pel que fa al tractament de les dades personals i les normes relatives a la lliure circulació d'aquestes dades».

Així mateix, tal com disposa l'art. 2.1 RGPD:

> «Aquest reglament s'aplica al tractament totalment o parcialment automatitzat de dades personals, i també al tractament no automatitzat de dades personals contingudes o destinades a ser incloses en un fitxer.»

A continuació aprofundim en els elements esmentats per a conèixer l'abast de la norma:

1) Persones físiques:

Les persones físiques són les úniques que són objecte de la tutela que proporciona el RGPD. Queden excloses d'aquesta protecció les persones jurídiques: una empresa, una associació, una fundació o bé l'administració pública.

El RGPD no contempla les dades relatives a les persones mortes. L'art. 3 de la LO 3/2018, de 5 de desembre, de Protecció de dades personals i garantia dels drets digitals (LOPDGDD), fa referència a aquesta qüestió.

LOPDGDD

La LO 3/2018, de 5 de desembre, de Protecció de dades personals i garantia dels drets digitals (LOPDGDD) va publicar-se en el BOE núm. 294 de 6 de desembre de 2018.

2) Dada personal:

> «Tota informació sobre una persona física identificada o identificable ("l'interessat"); es considerarà persona física identificable tota persona la identitat de la qual es pugui determinar, directament o indirectament, en particular mitjançant un identificador, com ara 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.» (Art. 4.1 RGPD)

Per tant: (a) Tota informació (b) relativa a una persona física identificada o identificable.

a) Tota informació: tant en un sentit objectiu (fets) com subjectiu (opinions). Tant la informació sensible (dades de salut), com aquella que no ho és. Tampoc és rellevant el fet que sigui feta pública, ni cal que sigui «secreta»; per tant, pot

tractar-se d'informació coneguda per molts (nom, adreça postal o de correu electrònic...). És indiferent a quin àmbit afecta: el personal o el professional. Tampoc té importància el format o el suport en el qual es contingui la informació –alfabètic, numèric, gràfic, fotogràfic, sonor o en suport paper. Per al dret a la protecció de dades no hi ha dades innòcues ni irrellevants.

b) Relativa a una persona **física identificada o identificable**: la qüestió és determinar si a partir de la informació disponible és possible distingir una persona entre un grup. Pel que fa a identificadors, l'art. 4.1 RGPD fa referència a:

> «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».

Les normes del RGPD no serien aplicables a les dades anònimes. Aquest supòsit s'ha de distingir de la **pseudonimització** (art. 4.5 RGPD), en què les dades personals es tracten de manera que no es puguin atribuir a una persona concreta sense utilitzar informació addicional. No obstant això, en el cas de dades pseudonimitzades continuen essent dades personals i és aplicable el RGPD.

Quant al terme de *dades personals*, cal tenir en compte:

a) La legislació distingeix, entre les dades personals, unes que qualifica com a *categories especials de dades* (art. 9 RGPD) i que tradicionalment es consideren dades sensibles. Es tracta de les dades que revelen:

> «L'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques, o l'afiliació sindical, i el tractament de dades genètiques, dades biomètriques adreçades a identificar de manera unívoca una persona física, dades relatives a la salut o dades relatives a la vida sexual o l'orientació sexual d'una persona física.» (Art. 9.1 RGPD)

El tractament d'aquestes dades està subjecte en alguns casos a un règim específic (per exemple, respecte al consentiment).

b) Una altra categoria que s'ha de tenir present és la relativa a les dades respecte a condemnes i infraccions penals, que tenen unes peculiaritats quant al seu tractament (art. 10 RGPD).

També cal tenir en compte:

c) Dades genètiques: art. 4. 13 RGPD.

d) Dades biomètriques: art. 4. 14 RGPD.

Consultes recomanades

Podeu consultar els dictàmens següents del Grup de l'art. 29:

Dictamen 4/2007 (WP 136), del 20 de juny del 2007, sobre el concepte de dades personals.

Dictamen 5/2014 (WP 216), del 10 d'abril, sobre tècniques d'anonimització.

3) Tractament:

> «qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, per procediments automatitzats o no, com la recollida, el registre, l'organització, l'estructuració, la conservació, l'adaptació o la modificació, l'extracció, la consulta, la utilització, la comunicació per transmissió, la difusió o qualsevol altra forma d'habilitació d'accés, confrontació o interconnexió, limitació, supressió o destrucció.» (Art. 4.2 del RGPD)

S'hi inclou tant el tractament automàtic com el no automàtic, en aquest últim cas, en la mesura que les dades siguin destinades a ser incloses en un fitxer.

Exemples de tractaments efectuats en paper als quals és aplicable el RGPD

Resultats mèdics, currículums en format paper, fulls de nòmina, expedients de clients, tot plegat ordenat alfabèticament sempre que les dades personals constin en un fitxer o estiguin destinades a ser-hi incloses (considerant 15 RGPD) perquè, per exemple, estan ordenades alfabèticament.

Cal tenir en compte que determinats tractaments, tot i afectar dades personals, queden exclosos de l'àmbit d'aplicació del RGPD, com s'explica més endavant.

1.1.2. En funció de l'àmbit territorial

Tal com disposa l'art. 3.1 RGPD:

> «Aquest Reglament s'aplica al tractament de dades personals en el context de les activitats d'un establiment del responsable o de l'encarregat a la Unió, independentment que el tractament tingui lloc a la Unió o no.»

El criteri que determina l'aplicació de la norma europea és el criteri de l'existència d'un establiment a la UE, amb independència del lloc en el qual es porta a terme el tractament.

Però, el RGPD va més enllà i en disposa l'aplicació fins i tot quan el responsable del tractament (RT) no estigui establert a la Unió en dos supòsits importants (art. 3.2 RGPD):

1) quan s'ofereixin béns o serveis a les persones interessades a la Unió, amb independència de si es requereix o no pagament;

2) quan es controla el comportament dels afectats, en la mesura que tingui lloc a la Unió.

Es tracta dels supòsits en què empreses (RT) que tenen la seu fora de la UE i, per tant, en principi no estarien subjectes al RGPD, ofereixen béns o serveis (per exemple de missatgeria, d'accés a continguts digitals), o venen béns a interessats a la Unió.

D'altra banda, es fa referència a l'observació del comportament dels interessats, concretament si les persones físiques són objecte d'un seguiment a internet, s'elaboren perfils, s'analitzen o prediuen les preferències personals, comportaments i actituds dels afectats (per exemple, es duen a terme pràctiques de publicitat personalitzada).

La finalitat d'aquesta disposició és que les persones físiques no siguin privades de la protecció a la qual tenen dret en virtut del RGPD. Per a determinar l'aplicació d'aquest es té en compte si l'RT projecta oferir serveis a interessats en un estat o diversos dels estats membres de la Unió. Aquest extrem, com ha dictaminat el TJUE, s'analitza tenint en compte elements com la llengua de la pàgina web des de la qual s'ofereix el bé o servei, la moneda utilitzada en el pagament o el lloc del lliurament dels béns.

1.2. Quan no s'aplica el RGPD?

El RGPD no s'aplica a determinats tractaments previstos en l'art. 2.2. RGPD.

L'excepció més important és la que es coneix com l'«excepció domèstica», de manera que el RGPD no s'aplica al tractament de dades personals «efectuat per una persona física en l'exercici d'activitats exclusivament personals o domèstiques» (art. 2.2.c RGPD).

> «Entre les activitats personals o domèstiques cal incloure la correspondència i l'administració d'un repertori d'adreces, o l'activitat a les xarxes socials i l'activitat en línia realitzada en el context de les activitats esmentades. No obstant això, aquest Reglament s'aplica als responsables o encarregats del tractament que proporcionin els mitjans per a tractar dades personals relacionades amb aquestes activitats personals o domèstiques.» (considerant 18 RGPD)

Això té una sèrie de conseqüències pel que fa als usuaris de les xarxes socials perquè quan es tracta d'un individu (particular) que les fa servir per a relacionar-se amb els amics o familiars, el tractament de dades personals que dugui a terme queda exclòs de l'àmbit d'aplicació del RGPD i, per tant, de les obligacions que s'hi estableixen. En canvi, lògicament, el responsable del tractament, el responsable d'aquesta xarxa social, sí que queda sota l'àmbit d'aplicació del RGPD.

En canvi, si es tracta d'una empresa o associació que fa ús d'una xarxa social per a promocionar els seus serveis (encara que siguin gratuïts), sí que és aplicable el RGPD.

1.3. Principis de protecció de dades (art. 5 RGPD)

Els primers textos normatius que regulaven el tractament de la informació personal van recollir uns principis que van establir unes directrius sobre com tractar les dades personals. Aquests principis s'han anat consolidant i constitueixen les línies mestres del tractament de la informació personal.

L'article 5 RGPD recull quins són els principis de protecció de dades. Constitueix una novetat del RGPD la introducció del principi de responsabilitat proactiva (art. 5.2 RGPD). A continuació s'enumeren i s'analitzen sumàriament aquests principis.

1) Principi de «licitud, lleialtat i transparència»

Tal com disposa l'article 5.1.a) RGPD, les dades personals han de ser:

> «a) tractades de manera lícita, lleial i transparent en relació amb l'interessat ("licitud, lleialtat i transparència").»

Aquests termes estan molt interconnectats. S'ha d'informar especialment sobre la identitat del responsable del tractament i de les seves finalitats, en definitiva, què es farà amb les dades. A més, el principi de transparència està lligat a l'exercici de tots els drets.

El deure d'informar es desenvolupa en els art. 12, 13 i 14 RGPD. El principi de licitud es concreta en l'art. 6 RGPD. Aquest precepte regula els supòsits que permeten que es dugui a terme un tractament de dades.

2) Principi de «limitació de la finalitat»

L'article 5.1 RGPD disposa que les dades personals han de ser:

> «b) recollides amb unes finalitats determinades, explícites i legítimes, i no seran tractades ulteriorment de manera incompatible amb aquestes finalitats; d'acord amb l'article 89, apartat 1, el tractament ulterior de les dades personals amb finalitats d'arxiu en interès públic, finalitats d'investigació científica i històrica, o finalitats estadístiques no es considera incompatible amb les finalitats inicials ("limitació de la finalitat").»

És a dir, en demanar les dades s'haurà de determinar la finalitat, per exemple, per a dur a terme una campanya publicitària de cotxes. En la mesura que l'afectat ha estat informat i ha donat el consentiment per a aquesta finalitat, les dades no podrien utilitzar-se per a demanar-li que es faci soci d'una ONG.

3) Principi de «minimització de les dades»

L'article 5.1 RGPD disposa que les dades personals han de ser:

> «c) adequades, pertinents i limitades al que és necessari en relació amb les finalitats per a les quals són tractades ("minimització de dades").»

Això comporta que, en dur a terme un tractament, s'hagi de valorar en primer lloc si efectivament cal tractar dades personals. En cas que s'hagin de tractar, aquest tractament ha de ser l'imprescindible per a la finalitat que es vol aconseguir.

> Per exemple, si es recullen dades per a una targeta d'accés a un gimnàs, hi ha dades com el nom i cognom, número de compte on domiciliar el pagament, adreça postal, adreça de correu electrònic i telèfon que pot considerar-se adequat sol·licitar. No obstant això, no compliria el principi de minimització demanar dades relatives a llocs preferits de vacances o conviccions religioses. En tot cas, si es demanessin aquestes altres dades, hauria de quedar molt clar que l'afectat no està obligat a proporcionar-les per a fer-se soci d'un gimnàs.

4) Principi d'«exactitud»

L'article 5.1 disposa que les dades personals han de ser:

> «d) exactes i, si cal, actualitzades; s'adoptaran totes les mesures raonables perquè se suprimeixin o rectifiquin sense dilació les dades personals que siguin inexactes respecte a les finalitats per a les quals es tracten ("exactitud").»

Les dades han de ser exactes i estar actualitzades. Altrament, han de rectificar-se o suprimir. Això també està relacionat amb el deure de l'RT de comunicar als destinataris de les dades que han estat rectificades / eliminades (art. 19 en relació amb l'art. 17 RGPD).

5) Principi de «limitació del termini de conservació»

L'article 5.1 RGPD disposa que les dades personals han de ser:

> «e) mantingudes de manera que es permeti la identificació dels interessats durant no més temps del necessari per a les finalitats del tractament de les dades personals; les dades personals es podran conservar durant períodes més llargs sempre que es tractin exclusivament amb finalitats d'arxiu en interès públic, finalitats d'investigació científica o històrica, o finalitats estadístiques, de conformitat amb l'article 89, apartat 1, sense perjudici de l'aplicació de les mesures tècniques i organitzatives apropiades que imposa aquest reglament per tal de protegir els drets i llibertats de la persona interessada ("limitació del termini de conservació").»

A les clàusules informatives s'ha d'informar del termini en què es pensa conservar les dades i, si no és possible fixar un termini, almenys establir els criteris que permetran determinar el termini [art. 13.2.a) i 14.2.a) RGPD].

6) Principi d'«integritat i confidencialitat»

L'article 5.1 RGPD determina que les dades personals han de ser:

> «f) tractades de tal manera que es garanteixi una seguretat adequada de les dades personals, inclosa la protecció contra el tractament no autoritzat o il·lícit, i contra la seva pèrdua, destrucció o dany accidental, mitjançant l'aplicació de mesures tècniques o organitzatives apropiades ("integritat i confidencialitat").»

Les mesures que s'adoptin per a fer front als possibles riscos hauran de tenir en compte la naturalesa, el context i les finalitats del tractament, i també el risc que el tractament pugui comportar per als drets i les llibertats de les persones.

7) Principi de «responsabilitat proactiva»

L'article 5.2. RGPD disposa que:

> «El responsable del tractament serà responsable del compliment del que disposa l'apartat 1 i capaç de demostrar-ho ("responsabilitat proactiva").»

La novetat que introdueix el RGPD és la referència a «capaç de demostrar-ho», cosa que es coneix com a *accountability* i que pot traduir-se com a «responsabilitat proactiva».

Sobre la base d'aquesta responsabilitat proactiva, les organitzacions han de ser conscients de quina informació tracten i amb quina finalitat duen a terme el tractament, i han de planificar i dissenyar com han de complir les normes contingudes en el RGPD. A més, han de poder *acreditar*, quan se'ls exigeixi, que compleixen adequadament la normativa.

En definitiva, el RGPD estableix sobre l'RT la càrrega d'adoptar determinades mesures i estar en condicions de poder-ho demostrar.

1.4. Bases legals que permeten el tractament de DCP (art. 6 RGPD)

Per a poder tractar les dades personals cal que hi hagi una base legal, una raó que ho justifiqui. És a dir, en el marc de la UE, a diferència d'altres ordenaments jurídics (com el dels Estats Units), no poden tractar-se les dades sense més ni més perquè a algú li interessi o perquè sigui la seva voluntat.

L'art. 6 RGPD enumera quins són aquests supòsits que permeten tractar les dades, de manera que si no es dona una de les circumstàncies que preveu aquest article no es poden tractar les dades.

Segons disposa l'art. 6.1 RGPD «El tractament només serà lícit si es compleix almenys una de les condicions següents [...]»:

1) el «consentiment» de l'interessat

2) «l'execució d'un contracte en el qual l'interessat és part»

3) «compliment d'una obligació legal»

4) «protegir interessos vitals de l'interessat o d'una altra persona física»

5) «compliment d'una missió realitzada en interès públic / exercici de poders públics»

6) «la satisfacció d'interessos legítims perseguits pel responsable del tractament o per un tercer»

Allò més rellevant de l'art. 6 RGPD és que sense un d'aquests supòsits enumerats no és possible dur a terme un tractament. Si bé és cert que hi ha molts supòsits i quedaran pocs casos fora d'ells.

No obstant això, el fet que concorri un d'aquests supòsits és necessari però no suficient. Per a tractar les dades personals cal a més que es compleixi sempre amb els principis de protecció de dades ja exposats (art. 5 RGPD).

Per tant, per a poder tractar les dades cal complir amb: art. 5 + art. 6 RGPD.

Així ho va establir el TJUE, entre altres, en la sentència del 24 de novembre del 2011, en el cas ASNEF (C-468/10 i C-469/10).

1.4.1. El consentiment

Característiques del consentiment

L'article 4.11 RGPD proporciona una definició del consentiment segons la qual es tracta de:

> «Tota manifestació de voluntat lliure, específica, informada i inequívoca per la qual l'interessat accepta, mitjançant una declaració o una clara acció afirmativa, el tractament de dades personals que el concerneixen.»

Consulta recomanada

Al respecte, vegeu l'art. 6 LOPDGDD, que duu per títol *Tractament basat en el consentiment de l'afectat*.

Una gran part dels tractaments de dades es basen en el consentiment del subjecte afectat, i una de les formes que tenen els subjectes de ser conscients que un responsable tracta les seves dades és que aquest últim en sol·liciti el consentiment. No obstant això, el fet de proporcionar el consentiment s'ha convertit molt sovint en una cosa automàtica. Això comporta que el consentiment es proporciona la majoria de les vegades de manera automàtica, sense la plena consciència i voluntat de l'afectat. Per això s'han d'adoptar precaucions respecte al recurs generalitzat al consentiment.

> Penseu en les nombroses vegades en què per a instal·lar una app al mòbil o per a consultar una informació o accedir a un servei es demana el consentiment de l'afectat. Es dona el consentiment d'una manera mecànica, sense llegir tota la informació proporcionada, i amb l'única finalitat d'obtenir com més aviat el servei o el bé desitjat.

L'exteriorització del consentiment

L'article 4.11 RGPD determina que la manifestació de voluntat ha de ser inequívoca, mitjançant una declaració o una clara acció afirmativa. Per tant, es rebutja el silenci com a manera d'obtenir el consentiment de l'afectat.

Per exemple, l'afectat rep una comunicació en què se li proposa subscriure's gratuïtament a una publicació i se li indica que si no contesta en un determinat termini s'entendrà que consent el tractament de determinades dades. D'acord amb l'article 4.11 RGPD, aquesta clàusula, juntament amb la manca de resposta de l'afectat, no tindria cap validesa com a consentiment. Per tant, en cas que una persona no manifesti res davant la sol·licitud de tractar les dades que l'afecten, això no comporta en cap cas que consenti el tractament.

Categories especials de dades. Com ja s'ha indicat en analitzar el terme dada, la gran majoria de textos legals que regulen el tractament de dades personals estableixen una distinció entre tipus de dades, de manera que es considera que determinada informació ha de gaudir d'una major protecció. El RGPD distingeix les que qualifica de «categories especials de dades». Per a tractar aquestes dades s'exigeix que el consentiment sigui explícit (art. 9.2.a. RGPD).

Condicions per a l'atorgament del consentiment

1) «Quan el tractament es basi en el consentiment de l'interessat, el responsable haurà de ser capaç de demostrar que l'afectat va consentir el tractament de les seves dades personals» (art. 7.1 RGPD). En definitiva, correspon a l'RT acreditar l'existència del consentiment.

2) Quan es demani el consentiment per a tractar dades, juntament amb altres assumptes, s'ha de distingir clarament la sol·licitud per al tractament de dades dels altres supòsits. S'ha d'emprar «un llenguatge clar i senzill» (art. 7.2 RGPD).

Aquest precepte determina que entre les diferents clàusules d'un formulari o document, s'identifiqui i separi clarament la relativa al tractament de les dades personals. La finalitat és que el subjecte pugui conèixer clarament allò que es demana i consentir una clàusula i, per exemple, rebutjar-ne una altra.

> Per exemple, es contracta un servei de telefonia i en el contracte s'han de distingir les clàusules que afecten la prestació del servei (les tarifes) de les que fan referència al tractament de dades (quines dades són necessàries, termini de conservació). Molt sovint la informació està barrejada i l'afectat no sap què consent.

3) «L'interessat té dret a retirar el consentiment en qualsevol moment» (art. 7.3 RGPD).

4) L'execució d'un contracte o la prestació d'un servei no pot vincular-se a l'obtenció de dades que no són necessàries per a proporcionar aquest bé o servei (art. 7.4 RGPD). Amb això es vol garantir que el consentiment sigui lliure, no condicionat al fet que si no es proporcionen determinades dades, no s'obtindrà un bé o servei.

És a dir, en la contractació d'un bé o servei, òbviament són necessàries determinades dades que caldrà demanar / proporcionar (per exemple, nom, adreça, DNI), però no exigir-ne d'altres no necessàries per al contracte en qüestió (com ara hàbits alimentaris o si l'afectat practica una determinada religió).

> Si es compra un bitllet d'avió, s'han de donar les dades relatives al nom, adreça de correu electrònic o DNI. Però, no es podria supeditar l'emissió del bitllet al fet que l'afectat proporcioni dades sobre els seus hàbits alimentaris o creences religioses.

El consentiment dels menors

El RGPD fa unes referències específiques al tractament de dades dels menors.

L'article 8 RGPD disposa que per a tractar les dades personals d'un menor d'edat, en relació amb l'oferta de serveis de la societat de la informació, si es vol obtenir el consentiment del menor, cal que tingui com a mínim setze anys.

> «Si el nen és menor de 16 anys, aquest tractament només es considera lícit si el consentiment el va donar o va autoritzar el titular de la pàtria potestat o tutela sobre el nen, i només en la mesura que es va donar o autoritzar.» (art. 8.1 RGPD)

No obstant això «els estats membres poden establir per llei una edat inferior per a aquestes finalitats, sempre que no sigui inferior per a tretze anys» (art. 8.2 RGPD). Aquest és el cas de l'Estat espanyol, que en l'art. 7 de la LOPDGDD determina, com a regla general, que «el tractament de les dades personals d'un menor d'edat únicament podrà fonamentar-se en el seu consentiment quan sigui major de catorze anys» (art. 7.1 PLOPD). En el cas de menors de 14 anys només serà lícit el tractament si hi consta el consentiment del titular de la pàtria potestat o tutela (art. 7.2 LOPDGDD).

L'RT ha de fer els:

> «esforços raonables per a verificar en aquests casos que el consentiment va ser donat o autoritzat pel titular de la pàtria potestat o tutela sobre el nen, tenint en compte la tecnologia disponible.» (art. 8.2 RGPD)

1.4.2. L'interès legítim (art. 6.1.f. RGPD)

1) Per a determinar quins interessos prevalen s'han de tenir en compte les expectatives raonables dels interessats.

2) Supòsits en què es pot donar aquest interès legítim:

a) quan hi hagi una relació entre afectat i responsable: per exemple si «l'interessat és client o està al servei del responsable» (considerant 47 RGPD)

b) «tractament de dades amb finalitats de màrqueting directe» (considerant 47 RGPD)

c) la transmissió de dades entre «responsables que formen part d'un grup empresarial» (considerant 48 RGPD)

d) «per a garantir la seguretat de la xarxa i de la informació» (considerant 49 RGPD)

3) «L'existència d'un interès legítim requeriria una avaluació acurada» (considerant 47 RGPD).

4) Aquesta base jurídica no serà aplicable al tractament efectuat per les autoritats públiques en l'exercici de les seves funcions (art. 6.1.f. *in fine* i considerant 47 RGPD).

5) En els supòsits en què l'afectat sigui un nen, la ponderació entre els interessos existents es decanta encara més a favor de l'afectat.

Lectures recomanades

Vegeu el Dictamen del Grup de l'Article 29, 6/2014 (WP 217), del 9 d'abril del 2014, sobre el concepte d'interès legítim.

Vegeu també la STJUE en el cas ASNEF (ja citat) i la STJUE cas Google, STJUE (Gran Sala), del 13 de maig del 2014, Google Spain, S. L., Google Inc. i Agència Espanyola de Protecció de Dades (AEPD), Mario Costeja González (C-131/12).

1.5. Els subjectes que participen en el tractament de dades

Quant a l'àmbit subjectiu, cal distingir entre els subjectes que **participen en el tractament** i els que el **supervisen** (les autoritats de protecció de dades i el DPO).

1.5.1. Els subjectes que tracten les dades personals

En tot tractament de dades els subjectes que sempre hi participen són: el responsable del tractament i l'afectat o interessat. Així mateix, en la majoria dels casos també hi ha l'encarregat o sotsencarregat i els destinataris de les dades (o tercers).

Responsable del tractament (RT)

L'article 4.7 RGPD estableix que el «responsable del tractament» o «responsable» és «la persona física o jurídica, autoritat pública, servei o un altre organisme que, sol o juntament amb altres, **determini les finalitats i mitjans del tractament**».

Per tant, allò que caracteritza l'RT és el fet de prendre una decisió, és a dir, determinar les finalitats i els mitjans del tractament.

En el cas en què hi hagi més d'un RT, els subjectes «són considerats corresponsables del tractament» (art. 26 RGPD).

Pel que fa a les funcions que porta a terme l'RT, es poden agrupar tenint en compte bàsicament tres moments: quan s'inicia o projecta el tractament, en efectuar-lo i quan finalitza.

En el marc anterior al RGPD, abans d'iniciar un tractament calia notificar-ho a l'autoritat de control. En el marc del RGPD, pot procedir-se al tractament, si bé l'RT ha de prendre una sèrie de prevencions i assegurar-se que compleix amb la normativa i ha de poder acreditar que això és així (principi de responsabilitat proactiva, ex art. 5.2 RGPD).

L'RT no té un xec en blanc per a tractar les dades de qualsevol manera, sinó que abans de dur a terme un tractament n'ha de valorar, pensar, estudiar la conveniència i la manera de dur-lo a terme d'acord amb la normativa i, especialment, els principis de protecció de dades.

Quan sigui necessari, ha de portar a terme una valoració de l'impacte que el tractament pot comportar per a la privacitat (*privacy impact assessment*) (art. 35 RGPD) i implementar des d'un primer moment mesures de privacitat basades en el disseny (art. 25 RGPD) i, en segons quins casos, fer una consulta prèvia a l'autoritat de control (art. 36 RGPD).

D'altra banda, cal que dugui a terme un «registre de les activitats de tractament» (art. 30 RGPD).

Per a això, haurà de dotar-se dels mitjans tècnics i personals adequats. I durant el tractament també haurà d'adoptar una sèrie de garanties i, especialment, dotar-se de les mesures de seguretat necessàries.

El conjunt de les obligacions que corresponen a l'RT són definides per aquesta nova perspectiva a la qual s'ha fet referència de la responsabilitat proactiva.

En definitiva, el responsable del tractament ha d'assegurar-se que compleix amb la normativa de protecció de dades i estar en condicions de poder-ho demostrar.

En conseqüència, tot això implica:

1) Abans d'iniciar el tractament:

a) verificar que es compleix amb la normativa de protecció de dades,

b) respectar els principis de protecció de dades,

c) verificar si el tractament és lícit (hi ha un fonament legal per a efectuar-lo),

d) quan calgui, dur a terme una valoració de l'impacte que pot tenir, respecte a la privacitat, el tractament de dades que es vol realitzar (*privacy impact assessment*),

e) quan sigui procedent, fer la consulta prèvia a l'autoritat de protecció de dades,

f) dotar-se dels mitjans tècnics i personals adequats, i

g) en cas de triar encarregats del tractament, fer-ho amb la diligència adequada i formalitzar un contracte o un altre negoci jurídic.

El RGPD també estableix el principi de *data protection by design* i *data protection by default*. S'han d'establir mesures tecnològiques que afavoreixin la privacitat des del primer moment de la concepció d'un producte/servei.

2) Durant el tractament:

a) adoptar una sèrie de garanties,

b) portar un registre de les activitats de tractament (art. 30.1 RGPD),

c) dotar-se dels mitjans tècnics i personals adequats,

d) si no s'ha fet a la fase anterior, elegir els encarregats del tractament amb la diligència adequada i subscriure un negoci jurídic,

e) adoptar les mesures de seguretat necessàries,

f) complir amb les obligacions pròpies del responsable,

g) donar resposta a l'exercici dels drets de l'afectat/interessat, i

h) poder demostrar que es compleix amb la normativa (principi de responsabilitat).

3) En finalitzar el tractament:

a) determinar si s'han de suprimir les dades o bé limitar-ne el tractament,

b) fer front al possible exercici d'accions de l'afectat / interessat,

c) valorar si es posa fi a la relació amb l'ET i valorar com s'hi posa fi, i

d) aplicar mesures tècniques i organitzatives per a demostrar que el tractament és conforme amb el reglament.

Per a això, quins elements ha de tenir en compte? Cal tenir «en compte la natura, l'àmbit, el context i les finalitats del tractament, els riscos de diversa probabilitat i gravetat que comporta el tractament» (art. 24.1 RGPD), i també «l'estat de la tècnica» i «el cost de l'aplicació» d'aquestes mesures (art. 25.1 RGPD).

Entre les obligacions concretes del responsable del tractament destaquen les següents:

1) Portar un registre (art. 30 RGPD), que ha de contenir la informació indicada en l'art. 30.1 RGPD. El registre ha de constar per escrit (art. 30.3 RGPD) i posar-se a disposició de l'autoritat de control (art. 30.4 RGPD).

Aquestes obligacions «no s'apliquen a cap empresa ni organització que ocupi menys de 250 persones si no és que el tractament pugui comportar un risc» (art. 30.5 RGPD).

2) Cooperar amb l'autoritat de control quan ho sol·liciti (art. 31 RGPD).

3) Deures relacionats amb la seguretat. L'RT ha d'identificar els riscos del tractament per a establir mecanismes adequats de processament de la informació.

Es té en compte un doble nivell d'aproximació des del risc. Algunes obligacions **només són aplicables a les activitats que comporten un risc elevat**. S'estableixen obligacions com la de dur a terme un *data protection impact assessment*, el deure de notificar als afectats les violacions de la seguretat de les dades o la consulta prèvia a les autoritats de protecció de dades (APD), de les quals parlarem més endavant.

L'RG estableix un conjunt de pautes en relació amb el nivell de risc que el tractament de dades personals pot comportar.

Entre les mesures que estableix l'art. 32 RGPD cal destacar:

> «a) la pseudonimització i el xifrat de dades personals;
>
> b) la capacitat de garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament;
>
> c) la capacitat de restaurar la disponibilitat i l'accés a les dades de manera ràpida [...]
>
> d) un procés de verificació, avaluació i valoració regulars de l'eficàcia de les mesures tècniques i organitzatives per a garantir la seguretat del tractament.»

Una novetat introduïda pel RGPD és el deure de notificar les violacions de seguretat (art. 33 i 34 RGPD). Es distingeix entre:

a) el deure de notificar «una violació de la seguretat a l'autoritat de control» (art. 33) i

b) la «comunicació d'una violació de la seguretat a l'interessat» (art. 34).

Pel que fa a la notificació de la violació a l'autoritat de control:

a) L'RT la notificarà a l'autoritat de control sense dilació indeguda, com a molt tard 72 hores després de tenir constància de l'incident (llevat que aquesta violació no constitueixi un risc per als drets i les llibertats de les persones).

b) La notificació haurà de contenir la informació que estableix l'article 33.4 RGPD.

L'RT «documentarà qualsevol violació de la seguretat de les dades personals» (art. 33.5 RGPD).

L'altre supòsit el constitueix la comunicació de la violació de la seguretat a l'interessat.

Aquesta comunicació s'ha de fer quan sigui probable que «comporti un alt risc per als drets i llibertats de les persones» (art. 34.1 RGPD).

4) L'avaluació d'impacte relativa a la protecció de dades. En determinats supòsits s'ha de dur a terme una avaluació de l'impacte relativa a la protecció de dades (art. 35 RGPD).

En especial, en determinats casos:

> «a) avaluació sistemàtica i exhaustiva d'aspectes personals […], com l'elaboració de perfils […]; b) tractament a gran escala […] c) observació sistemàtica a gran escala d'una zona d'accés públic.»

La noció d'avaluació d'impacte relativa a la protecció de dades (art. 35 RGPD) és més coneguda per les sigles en anglès PIA (*privacy impact assessment*). El PIA s'ha de fer abans de dur a terme el tractament. Hi ha la possibilitat de dur a terme PIA per sectors (tractaments semblants que presenten un risc semblant).

5) Consulta prèvia. En determinats casos s'ha de fer una consulta prèvia (art. 36 RGPD).

6) Designació de l'encarregat del tractament (ET). L'RT, segons determina l'article 28 RGPD, triarà només un encarregat que ofereixi garanties suficients per a aplicar mesures tècniques i organitzatives apropiades. L'article 28.1 RGPD estableix una obligació general de diligència en la selecció de l'encarregat.

L'encarregat del tractament

L'encarregat del tractament (ET) o «encarregat» és «la persona física o jurídica, autoritat pública, servei o un altre organisme que tracti dades personals per compte del responsable del tractament» (art. 4.8 RGPD). Per tant, no és el subjecte que pren la iniciativa de tractar les DCP.

L'article 28.1 RGPD disposa que l'RT triarà un encarregat que ofereixi garanties suficients per aplicar mesures tècniques i organitzatives apropiades, de manera que el tractament sigui conforme amb els requisits del Reglament.

La relació entre RT i ET s'ha de regir per un contracte o un altre acte jurídic que vinculi l'encarregat respecte al responsable (art. 28.3 RGPD) que necessàriament ha d'establir «l'objecte, la durada, la natura i la finalitat del tractament, el tipus de dades personals i categories d'interessats, i les obligacions i drets del responsable».

L'article 28.3 RGPD disposa quin ha de ser el contingut d'aquest contracte o acte jurídic, és a dir com l'ET ha de tractar les dades personals. En qualsevol cas, l'ET no és un mer executor de les ordres de l'RT, ja que com disposa l'article 28.3. *in fine*, «l'encarregat informarà immediatament el responsable si, en la seva opinió, una instrucció infringeix el reglament o altres disposicions».

Cada encarregat «portarà un registre de totes les categories d'activitats de tractament efectuades per compte d'un responsable» (art. 30.2 RGPD). Aquest registre constarà per escrit i l'ET el posarà «a disposició de l'autoritat de control que ho sol·liciti» (art. 30.4 RGPD).

L'obligació de portar el registre no és exigible a determinades empreses o organitzacions (art. 30.5 RGPD).

La possibilitat que l'ET recorri a un altre ET (en definitiva, en subcontracti les funcions) està especialment contemplada en el RGPD. Això és possible si l'ET té l'autorització prèvia per escrit, específica o general, del responsable. Si un ET infringeix el reglament «en determinar les finalitats i mitjans del tractament», serà considerat RT (art. 28.10).

Qualsevol subjecte que tracti dades personals ho ha de fer amb una determinada diligència, d'acord amb els art. 5.1.f) i 29 RGPD.

En definitiva, pel que fa a la relació entre RT i ET, cal tenir en compte el següent:

1) L'ET fa un tractament per compte d'un responsable.

2) L'RT ha de triar qui ofereixi garanties suficients per a aplicar mesures tècniques i organitzatives apropiades.

3) L'ET no pot recórrer a un altre encarregat sense autorització prèvia i per escrit de l'RT.

4) La relació entre l'RT i l'ET es regeix per un contracte o acte jurídic, que ha d'establir, entre altres aspectes: l'objecte, la durada, la natura i la finalitat del tractament, el tipus de dades personals tractades, les categories d'interessats, i les obligacions i drets de l'RT.

5) El contracte o acte jurídic constarà per escrit, inclús en format electrònic.

6) La fi de la prestació implica esborrat o devolució de dades, sense incloure transferència a un altre encarregat, tret que així s'hagi estipulat expressament.

7) L'ET ha d'informar el responsable si, al seu entendre, una instrucció infringeix el RGPD.

Altres subjectes

El RGPD contempla la participació en el tractament d'altres subjectes. L'article 4.9) RGPD fa referència a la figura del **destinatari**.

Destinatari és:

> «La persona física o jurídica, autoritat pública, servei o un altre organisme al qual es comuniquin dades personals, tant si es tracta d'un tercer com si no. No obstant això, no es consideren destinataris les autoritats públiques que puguin rebre dades personals en el marc d'una investigació concreta de conformitat amb el Dret de la Unió o dels estats membres; el tractament de les dades per les autoritats públiques serà d'acord amb les normes en matèria de protecció de dades aplicables a les finalitats del tractament.»

Els subjectes afectats pel tractament

Es tracta dels subjectes afectats o interessats, als quals afecta el tractament de dades.

Entre les definicions que es recullen en l'article 4 RGPD, no n'hi ha una que faci referència a l'interessat o afectat. En qualsevol cas, es tracta de la persona a qui fa referència el tractament. Per a l'àmbit d'aplicació del RGPD ja s'ha subratllat que es tracta en tot cas d'un subjecte, persona física, i que, per tant, el RGPD no és aplicable a les persones jurídiques.

1.5.2. La supervisió del tractament

En aquest subapartat s'analitzen dos aspectes: les autoritats de protecció (APD) i el delegat de protecció de dades (DPD).

Les autoritats de protecció de dades

Les autoritats de protecció (APD), segons l'esquema del RGPD, constitueixen un pilar bàsic en la implementació del RGPD i aquest en reforça la tasca. Són regulades en el capítol VI del RGPD, que estableix les normes bàsiques d'actuació, la seva competència, funcions i poders, i en el capítol VII, que fa referència als mecanismes de cooperació i de coherència.

Segons l'article 4.21 GDPR, l'«autoritat de control» és «l'autoritat pública independent establerta per un estat membre d'acord amb el que disposa l'article 51».

Juntament amb les autoritats de protecció, es crea el Comitè Europeu de Protecció de Dades (art. 68 a 76), que substitueix el Grup de l'article 29, creat precisament per l'article 29 Directiva 95/46 i que ha desenvolupat una encomiable tasca d'interpretació i d'aclariment de l'articulat de la directiva.

Un aspecte al qual ha tractat de donar resposta el RGPD és el cada vegada més gran tractament transfronterer de DCP (dins de la UE). Per a això, el RGPD ha previst una sèrie de mecanismes i un d'ells és el relatiu a la coordinació entre autoritats de protecció de dades. D'aquesta manera, les autoritats tenen determinats poders d'investigació en altres estats.

En els supòsits en què a causa del tractament transfronterer de dades puguin resultar competents diferents APD, s'ha de determinar quina n'és l'autoritat de control principal.

El RGPD estableix un complex sistema per a determinar quina autoritat és la competent per a decidir un assumpte, en virtut de si hi ha punts de connexió en un sol estat o en múltiples estats. També s'estableix un mecanisme de cooperació entre autoritats (art. 60 a 62).

Consulta recomanada

Pel que fa a autoritat de control interessada, vegeu article 4.22 RGPD.

En la mesura que les APD prenen decisions que poden afectar l'aplicació uniforme del reglament, s'estableix un procediment de coherència (art. 63 a 67).

El Comitè Europeu de Protecció de Dades

L'article 29 DPD va crear un grup de protecció de les persones respecte al tractament de dades personals, anomenat Grup de l'article 29, que té caràcter consultiu i independent. L'article 68 RGPD crea el Comitè Europeu de Protecció de Dades identificat com a «Comitè», com a organisme de la Unió, que gaudeix de personalitat jurídica i que substitueix el Grup de l'article 29.

En l'ordenament jurídic espanyol hi ha diferents autoritats de protecció de dades: l'Agència espanyola de protecció de dades, l'Autoritat catalana, l'Agència basca i l'organisme andalús per la transparència.

El delegat de protecció de dades

Una altra de les novetats introduïdes en el RGPD és la figura del delegat de protecció de dades (DPD). En el cas de les administracions públiques, la seva designació és obligatòria. Pel que fa a les empreses privades, depèn del tipus de tractament que duguin a terme.

Tal com disposa l'article 37 RGDP, «el responsable i l'encarregat del tractament han de designar un delegat de protecció de dades sempre que»:

1) «el tractament el porti a terme una autoritat o organisme públic»;

2) les activitats principals de l'RT o ET «consisteixin en operacions de tractament que [...] requereixin una observació habitual i sistemàtica d'interessats a gran escala», per exemple, aquest seria el cas de la videovigilància;

3) «consisteixin en el tractament a gran escala de categories especials de dades».

> «El delegat de protecció de dades serà designat atenent les seves qualitats professionals i, en particular, els seus coneixements especialitzats de Dret i la pràctica en matèria de protecció de dades, i la seva capacitat per a exercir les funcions indicades en l'article 39.» (art. 37.5)

El RGPD no regula quin tipus de titulació ha de tenir el subjecte que exerceixi les funcions de DPD. Per tant, qualsevol subjecte que tingui les qualitats i coneixements exigits en el RGPD pot exercir aquesta tasca professional. No obstant això, l'AEPD, per a dotar de més seguretat i facilitar l'acreditació d'aquests coneixements, ha establert un sistema de certificació de persones.

L'article 38 RGPD regula la posició del delegat de protecció de dades dins de l'administració, empresa o organització. S'ha de garantir que «participi de manera adequada i en el temps oportú en totes les qüestions relatives a la protecció de dades personals». El DPD té unes funcions mínimes, recollides en l'article 39.1 RGPD: informar i assessorar, «supervisar el compliment de la normativa, actuar com a punt de contacte amb l'autoritat de control i cooperar-hi».

1.6. Els mecanismes de *soft law*: els codis de conducta i la certificació

Ja s'ha assenyalat que un dels principis sobre els quals es basa el RGPD i que implica una novetat de la nova regulació és el principi de responsabilitat proactiva.

Això està lligat a una sèrie de mesures que es poden qualificar com a *soft law* i que es concreten en la realització de PIA (*privacy impact assessment*), als quals ja s'ha fet referència, l'adopció de codis de conducta i la implementació de mecanismes de certificació.

Aquests mecanismes constitueixen eines per a fer efectiu el principi de responsabilitat proactiva.

Els **codis de conducta** tenen com a objectiu conduir a l'aplicació correcta del RGPD.

Les **certificacions, segells i marques** ajuden a demostrar que es compleix amb les disposicions del RGPD (es tracta, en definitiva, de mecanismes de *compliance*), és a dir d'acreditar el compliment del RGPD.

Les organitzacions independents de certificació, o bé les APD o CEPD (Comitè europeu de protecció de dades), certifiquen les empreses i supervisen el compliment adequat de la certificació. És a dir, duen a terme un seguiment del fet que l'empresa en qüestió compleix i s'adequa a allò que ha estat certificat. Això també representa una novetat del RGPD respecte a la directiva.

1.6.1. Els codis de conducta

Els codis de conducta constitueixen un mecanisme d'autoregulació (*self-regulatory instrument*), l'eficàcia del qual depèn en part del nivell de ratificació que rep de les APD o altres autoritats.

Tal com disposa l'art. 40.1 RGPD, «les associacions i altres organismes representatius de categories de responsables o encarregats del tractament poden elaborar codis de conducta o modificar aquests codis» per tal d'especificar l'aplicació del RGPD.

1.6.2. La certificació

En el marc del RGPD es tracta d'un mecanisme establert sota l'escrutini directe / indirecte de l'APD competent. Una certificació pot ser emesa per un ens certificador (en funció dels criteris adoptats per l'APD) o per la mateixa APD.

> «La certificació és voluntària i està disponible per mitjà d'un procés transparent.» (art. 42.3 RGPD)

La certificació no limita la responsabilitat de l'RT o ET pel que fa al compliment del reglament «i s'entén sense perjudici de les funcions i els poders de les autoritats de control que siguin competents» (art. 42.4 RGPD).

La certificació en virtut d'aquest article és expedida pels organismes de certificació ex article 43, per l'autoritat de control competent o pel Comitè de conformitat amb l'article 63 (art. 42.5 RGPD).

1.7. Els drets de l'afectat

El capítol III del RGPD es dedica als drets de l'interessat. Aquest capítol es divideix en cinc seccions que fan referència a «transparència i modalitats» (secció 1); «informació i accés a les dades personals» (secció 2); «rectificació i supressió» (secció 3); «dret d'oposició i decisions individuals automatitzades» (secció 4), i «limitacions» (secció 5).

Entre els drets reconeguts cal subratllar que se'n recullen de nous: el dret a la limitació del tractament i el dret a la portabilitat. Així mateix, el dret de cancel·lació passa a anomenar-se dret de supressió. D'altra banda, l'anomenat dret a l'oblit s'esmenta en l'article 17 RGPD.

1.7.1. Transparència i modalitats

La secció 1 del capítol III té per rúbrica «transparència i modalitats».

La informació que s'ha de proporcionar constitueix un pressupòsit per a poder exercir altres drets, com el dret de rectificació o supressió, o bé oposar-se a tractaments que comportin decisions individuals automatitzades.

La transparència es regula en l'article 12. La comunicació a l'interessat s'ha de fer:

> «de manera concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill, en particular qualsevol informació adreçada específicament a un nen.» (art. 12.1 RGPD)

L'RT facilitarà a l'interessat la informació relativa a les seves actuacions d'acord amb la sol·licitud presentada per l'afectat. En tot cas, en el termini d'un mes ha de donar resposta a l'afectat, termini que pot prorrogar dos mesos més en cas necessari, i informarà l'interessat d'aquestes pròrrogues (art. 12.3 RGPD). La informació facilitada per regla general ha de ser gratuïta.

Pel que fa al contingut concret de la informació que s'ha de proporcionar a l'interessat / afectat, el RGPD distingeix en funció de si les dades s'han obtingut de l'afectat o no.

Supòsits en què les dades s'obtenen de l'afectat (art. 13 RGPD). Es disposa que el contingut de la informació ha de fer referència a:

1) L'àmbit subjectiu (RT i DPD), destinataris o categories de destinataris i intenció de transferir les dades a un tercer país o organització internacional.

2) Quant al contingut concret, un aspecte rellevant és proporcionar informació de les finalitats del tractament i la base jurídica. L'article 13.2 disposa quina altra informació s'ha de proporcionar.

Supòsits en què les dades no s'obtenen directament de l'afectat. Juntament amb alguns aspectes similars als del punt anterior, l'article 14.2.f), que disposa la necessitat d'informar sobre «la font de la qual procedeixen les dades personals i, si escau, si procedeixen de fonts d'accés públic».

Estretament lligat a la informació és l'aspecte del seu accés, regulat en l'article 15 RGPD (**Dret d'accés de l'interessat**): sobre la base del dret d'accés l'interessat té dret a obtenir de l'RT «confirmació de si es tracten o no dades personals que el concerneixen i, en aquest cas, dret d'accés a les dades personals» i a la informació que preveu l'article 15.1 RGPD.

1.7.2. Rectificació i supressió

Tal com disposa l'article 16:

> «L'interessat té dret a obtenir sense dilació indeguda del responsable del tractament la rectificació de les dades personals inexactes que el concerneixin. Tenint en compte les finalitats del tractament, l'interessat té dret que es completin les dades personals que siguin incompletes, inclusivament mitjançant una declaració addicional.»

L'objectiu d'aquest dret és doncs que s'actualitzin les dades o que es completin.

L'article 17 es dedica al dret de supressió («el dret a l'oblit»). Segons aquest precepte (art. 17.1), «l'interessat té dret a obtenir sense dilació indeguda del responsable del tractament la supressió de les dades personals que el concerneixin, el qual està obligat a suprimir sense dilació indeguda les dades personals quan es doni alguna de les circumstàncies següents: **a)** Les dades personals ja no són necessàries»; «**b)** L'interessat retira el consentiment»; «**c)** L'interessat s'oposa al tractament»; «**d)** Les dades personals han estat tractades il·lícitament»; «**e)** s'han de suprimir per al compliment d'una obligació legal»; «**f)** s'han obtingut en relació amb l'oferta de serveis de la societat de la informació» a nens.

Vegeu també

Aquest dret s'analitza de manera més detallada en l'apartat 2 (Dret a l'oblit) d'aquest mòdul.

1.7.3. Dret a la limitació del tractament

Es tracta d'un nou dret (art. 18 RGPD), en virtut del qual «l'interessat té dret a obtenir del responsable del tractament la limitació del tractament de les dades» (art.18.1) quan es compleixin determinades condicions. La principal diferència respecte del bloqueig de les dades és que no es tracta d'una obligació, sinó d'un dret de l'interessat.

Se'n distingeix un ventall de supòsits. Uns són equivalents a la cancel·lació cautelar (cf. impugnar exactitud de dades), si bé cautelarment s'han de conservar.

1.7.4. El dret a la portabilitat de les dades

Aquest dret està reconegut a l'article 20 RGPD. Sobre la base d'aquest article (art. 20.1) «l'interessat té dret a rebre les dades personals que li incumbeixin, que hagi facilitat a un responsable del tractament, en un format estructurat, d'ús comú i lectura mecànica, i a transmetre'ls a un altre responsable del tractament sense que ho impedeixi el responsable a qui els hagués facilitat» en els supòsits que contempla l'article 20 RGPD.

En exercir aquest dret l'interessat té dret a què les dades personals es transmetin directament de responsable a responsable quan sigui tècnicament possible.

> «El dret a la portabilitat no afectarà negativament els drets i llibertats d'altres.» (art. 20.4 RGPD)

Constitueix una novetat important, com un complement del tradicional dret d'accés. Es tracta del dret de rebre les dades que incumbeixen a un interessat.

Una de les qüestions que planteja aquest dret és determinar fins on arriba.

Què s'ha d'entendre per *dades que l'afectat ha facilitat* a un RT? Això pot ser discutible. Es considera que les dades no s'han de limitar a les que han estat facilitades per l'afectat, sinó també altres en què l'activitat amb l'interessat dona lloc a un tractament de dades, per exemple, dades de navegació de l'interessat.

1.7.5. Dret d'oposició i decisions individuals automatitzades

L'article 21 RGPD regula el dret d'oposició. Hi ha dos grans supòsits en què es pot exercir aquest dret:

1) L'article 21.1 RGPD regula l'exercici del dret d'oposició per motius fundats en una situació particular.

Es tracta dels casos en què les dades es processen sobre la base dels articles 6.1.e) o f) RGPD. En aquests casos l'interessat té dret a oposar-se en qualsevol moment al tractament al·legant l'existència d'una situació particular.

La petició de l'afectat ha de motivar-se. Si preval l'exercici del dret d'oposició, l'RT ha de deixar de tractar les dades llevat que acrediti que hi ha motius legítims imperiosos per al tractament que prevalguin sobre els interessos, els drets i les llibertats de la persona interessada.

2) L'article 21.2. contempla l'exercici del dret d'oposició «quan el tractament de dades personals tingui per objecte el màrqueting directe». En aquestes circumstàncies «l'interessat té dret a oposar-se en tot moment al tractament de les dades personals que el concerneixin, incloent-hi l'elaboració de perfils». «Quan l'interessat s'oposi al tractament amb finalitats de màrqueting directe, les dades personals deixaran de ser tractades per a aquestes finalitats» (art. 21.3 RGPD).

L'article 22 RGPD fa referència a les «decisions individuals automatitzades» i l'elaboració de perfils. L'article 4.4 RGPD proporciona una definició de què es considera «elaboració de perfils»:

> «Tota forma de tractament automatitzat de dades personals consistent a fer servir dades personals per a avaluar determinats aspectes personals d'una persona física, en particular per a analitzar o predir aspectes relatius al rendiment professional, situació econòmica, salut, preferències personals, interessos, fiabilitat, comportament, ubicació o moviments d'aquesta persona física».

L'ingent i constant tractament massiu de dades afavoreix sens dubte l'adopció de decisions de manera automàtica, sense intervenció humana. Partint d'aquest tipus de decisions, una persona pot veure com se li denega un crèdit o es rebutja la sol·licitud presentada per a un lloc de treball sense que hi hagi aparentment un motiu. Així mateix, els tractaments massius poden comportar la inferència de conclusions errònies i ocasionar efectes discriminatoris.

En la mesura que aquestes decisions cada vegada són més generalitzades, el legislador disposa mesures per a controlar l'ús que se'n pugui fer.

La regla general és que «tot interessat té dret a no ser objecte d'una decisió basada únicament en el tractament automatitzat, incloent-hi l'elaboració de perfils, que produeixi efectes jurídics en ell o l'afecti significativament de manera semblant» (art. 22.1 RGPD). No obstant això, aquest dret també reconeix algunes excepcions (art. 22.2 RGPD).

1.8. Limitacions

L'exercici dels drets recollits en el capítol III està subjecte a una sèrie de limitacions, tal com disposa l'article 23 RGPD.

Es pot limitar l'abast dels drets i obligacions establerts en el RGPD, per mitjà de mesures legislatives, i sempre que es tracti d'una «mesura necessària i proporcionada en una societat democràtica» per a salvaguardar una sèrie de béns, com ara, entre altres, la seguretat de l'estat, la defensa, la seguretat pública o bé la prevenció, investigació, detecció o enjudiciament d'infraccions penals, o l'execució de sancions penals (art. 23.1).

1.9. Transferències internacionals de dades

Actualment hi ha un flux transfronterer constant de dades, tant dins de la Unió Europea com fora d'ella. El règim de protecció de dades de la UE va tenir ja des dels seus inicis com a objectiu garantir la lliure circulació de dades en el mercat interior mitjançant l'harmonització de la normativa de la UE. Les transmissions de dades fora de la UE es coneixen com a transferències internacionals de dades.

Una transferència internacional de dades és un tractament de dades que comporta una transmissió de dades **fora del territori de l'Espai Econòmic Europeu (EEE)**, tant si constitueix una cessió o comunicació de dades, com si té per objecte la realització d'un tractament de dades (fora de la UE) per compte del responsable del fitxer establert en territori d'un dels estats membres de la Unió Europea.

La regla general és que es prohibeix la transferència de dades a tercers països que no ofereixin un nivell adequat de protecció. No obstant això, s'estableixen supòsits en què es permet la transmissió:

1) En els casos en què hi hagi una decisió d'adequació prèvia de la Comissió Europea, segons els requisits de l'article 45 RGPD.

2) Quan no hi hagi una decisió d'adequació, mitjançant l'establiment de garanties adequades (art. 46 RGPD). Entre elles cal destacar les «normes corporatives vinculants» (art. 47 RGPD).

3) Que es donin algunes de les excepcions previstes en l'article 49 RGPD.

1.10. Responsabilitat i sancions

1.10.1. Responsabilitat administrativa

En els supòsits en què no es compleixi amb la normativa de protecció de dades, això pot comportar que s'imposin determinades sancions. Una de les novetats del RGPD és la imposició d'elevades sancions econòmiques, aspecte que igualarà els països de la UE. En el marc de la Directiva del 95 hi havia en aquest

àmbit importants divergències, de manera que hi havia països en què les sancions eren pràcticament inexistents mentre que en altres, com el cas espanyol, s'establien multes molt elevades.

L'article 83 RGPD porta per rúbrica: «Condicions generals per a la imposició de multes administratives». S'hi determina que cada autoritat de control ha de garantir que la imposició de les multes administratives «siguin en cada cas individual efectives, proporcionades i dissuasives» (art. 83.1).

«Les multes administratives s'han d'imposar en funció de les circumstàncies de cada cas individual» (art. 83.2) i per a decidir la imposició d'una multa administrativa i la seva quantia s'han de tenir en compte els elements recollits en l'article 83.2. a) a k).

En relació amb les quanties, s'ha de subratllar que s'estableix una quantitat que opera com una quantitat màxima, però també la sanció pot fixar-se sobre la base d'un determinat percentatge del volum de negoci total.

La tipificació de les sancions és la següent:

1) Multa de fins a 10 M € o per a empreses es pot establir fins al 2% de volum de negoci anual a escala mundial (s'opta per la de major quantia), quan s'infringeixin les disposicions que es contemplen en l'article 83.4 RGPD.

El règim sancionador en la LOPDGDD

Es troba regulat en els articles 70 a 78 d'aquesta norma. Es distingeix entre infraccions molt greus (art. 72), infraccions considerades greus (art. 73) i aquelles considerades lleus (art. 74).

2) Multa de fins a 20 M € o fins al 4%, en el supòsit d'incompliment de les disposicions previstes en l'art. 83.5 RGPD.

1.10.2. Responsabilitat civil (RC)

Cal no confondre el règim sancionador de caràcter administratiu dels altres supòsits en què, com a conseqüència de l'incompliment d'allò que disposa la norma, els interessats pateixin **un dany o lesió en els seus béns o drets**.

L'existència de danys origina un deure de rescabalar l'afectat (es tracta d'un supòsit de responsabilitat civil). Aquesta RC sorgeix quan l'existència del dany o lesió en els drets o béns de l'afectat és conseqüència de l'incompliment de la normativa. Per exemple, com a conseqüència de no adoptar les mesures de seguretat necessàries es perden una sèrie de dades que causen un perjudici econòmic a l'afectat.

El fet mateix de no adoptar determinades mesures de seguretat pot comportar una sanció. Si, a més, com a conseqüència d'aquesta manca de seguretat es produeixen danys econòmics a l'afectat (per exemple, algú entra en els seus comptes i en suplanta la identitat), aquesta conducta originaria així mateix el deure de rescabalar els perjudicis econòmics i morals ocasionats (responsabilitat civil).

Cal notar, a més, que el destinatari de la quantitat en què consisteixi la sanció econòmica o la indemnització és diferent en un cas i l'altre. Quan es produeix una infracció de la normativa de protecció de dades, la sanció (la multa) té com a destinatari l'Autoritat de protecció. Per contra, en el cas de produir-se un dany moral o econòmic, la quantitat en què consisteixi el rescabalament del dany té com a destinatari l'afectat.

En el RGPD, el dret a la indemnització i responsabilitat està regulat en l'article 82.1 RGPD, segons el qual:

> «Tota persona que hagi patit danys i perjudicis materials o immaterials com a conseqüència d'una infracció d'aquest reglament té dret a rebre del responsable o l'encarregat del tractament una indemnització pels danys i perjudicis soferts.»

Es tracta d'una responsabilitat objectiva, en la mesura que l'article 82.3 RGPD disposa que:

> «El responsable o encarregat del tractament està exempt de responsabilitat en virtut de l'apartat 2 si demostra que no és de cap manera responsable del fet que hagi causat danys i perjudicis.»

En la mesura que la responsabilitat civil i la responsabilitat administrativa obeeixen a finalitats diferents, poden concórrer totes dues o hi pot haver l'una sense l'altra.

2. Dret a l'oblit

Miquel Peguera

2.1. Introducció

Ens els darrers anys, l'expressió *dret a l'oblit* s'ha fet popular. Amb aquesta expressió se sol fer referència al dret d'eliminar de la xarxa informació sobre una persona, que aquesta mateixa o altres hagin pujat a internet. Es presenta sovint com un dret a no ser recordat a les xarxes, un dret a «ser oblidat». Naturalment, és una qüestió molt relacionada amb el dret a la protecció de dades. Com hem vist en els apartats anteriors, el titular de les dades personals té –en determinades circumstàncies– el dret de sol·licitar la supressió de les seves dades, o bé d'oposar-se al seu tractament, i aquestes són les vies per mitjà de les quals es pot fer efectiu aquest anomenat dret a l'oblit. El RGPD ha volgut recollir explícitament l'expressió «dret a l'oblit» –si bé només entre cometes i entre parèntesis– en l'article que tracta sobre el dret de supressió de dades. Així, la rúbrica de l'article 17 RGPD diu Dret de supressió («el dret a l'oblit»). De fet, ni el dret de supressió ni el d'oposició són nous. Ja estaven recollits, amb requisits similars, a la Directiva 95/46. Certament, però, el RGPD ha ampliat l'abast del dret de supressió amb una nova previsió que vol facilitar la cancel·lació de les dades que s'han anat multiplicant a les xarxes, com veurem al final d'aquest apartat (art. 17.2 RGPD).

Sovint, però, s'entén per dret a l'oblit una manifestació més concreta: la possibilitat de limitar l'ús dels cercadors d'internet per a obtenir informació sobre una persona.

Google i els altres cercadors indexen una enorme quantitat de continguts publicats al web. Si introduïm en el cercador el nom d'una persona, obtenim resultats que enllacen a diferents llocs on apareix informació referida a l'interessat. Aquestes informacions poden ser de molts tipus. A voltes es tracta de notícies antigues tretes de l'hemeroteca digital d'un diari, o d'entrades en blogs, o comentaris en xarxes socials. Pot ser que siguin informacions inexactes, o bé obsoletes o ja no rellevants en el moment actual. En tot cas, poden tenir un impacte greu en la persona interessada, especialment quan els primers resultats porten a informacions negatives ja oblidades, que queden així fora del seu context, i que poden perjudicar la imatge o el desenvolupament de la persona afectada.

Des de fa alguns anys, aquest tipus de situacions va dur a plantejar si el dret de protecció de dades, i en concret la Directiva 95/46, permetia a l'interessat reclamar directament al cercador que suprimís els resultats en qüestió. Després de múltiples resolucions dictades per l'Agència Espanyola de Protecció de

Dades (AEPD), que es van recórrer davant l'Audiència Nacional (AN), aquest darrer tribunal va plantejar la qüestió al Tribunal de Justícia de la UE (TJUE). El TJUE va dictar una sentència en què reconeix la possibilitat d'exigir als cercadors la supressió de determinats resultats. Es tracta del cas Google Spain, que examinem a continuació, en el qual es van posar les bases del dret a l'oblit en els cercadors d'internet.

2.2. El cas Google Spain

El 13 de maig del 2014, el TJUE va dictar sentència en l'assumpte C-131/12, Google Spain, S.L. i Google Inc. contra Agència Espanyola de Protecció de Dades (AEPD) i Mario Costeja González, conegut com a cas Google Spain. La persona afectada en el cas concret era l'advocat Mario Costeja. Fent una cerca pel seu nom a Google apareixia com un dels primers resultats un enllaç a un anunci oficial publicat al diari *La Vanguardia* l'any 1998, referit a l'execució d'immobles per deutes a la Seguretat Social. El tema ja havia estat solucionat anys enrere, i no tenia cap rellevància actual, però, tot i així, continuava apareixent en posar el seu nom al cercador.

El TJUE, aplicant la Directiva 95/46 i tenint en compte els drets a la privacitat i a la protecció de dades, reconeguts a la Carta de Drets Fonamentals de la UE, va concloure que l'interessat té dret, en determinades circumstàncies, a exigir la supressió de certs resultats en les cerques fetes a partir del seu nom.

La sentència va considerar que la indexació de les informacions i la seva presentació com a resultats de cerca són un tractament de dades personals. És un tractament diferent del que fa la font on es van publicar les dades inicialment, i el responsable d'aquest tractament és el cercador. Per tant, indica el tribunal:

> «l'interessat pot exercir els seus drets de protecció de dades davant el cercador, concretament els drets de cancel·lació i d'oposició, sense necessitat de adreçar-se prèviament a la font».

Atès que es tracta d'una reclamació basada en el dret a la protecció de dades, no és necessari acreditar que l'interessat ha sofert un dany com a conseqüència de l'aparició de la informació en els resultats de cerca. Tampoc no és necessari que la informació sigui falsa o il·lícita. Sí que cal, però, que concorrin els requisits per a l'exercici dels drets de supressió o de cancel·lació.

Concretament, el TJUE va indicar que:

> «l'interessat té el dret d'exigir al cercador que, quan es faci una cerca pel seu nom, no es mostrin a la llista de resultats enllaços que condueixin a dades que no compleixen amb el principis de qualitat o licitud de dades perquè siguin, per exemple, inadequades, no pertinents irrellevants o excessives».

Ara bé, l'interessat no tindrà aquest dret quan la informació sigui d'interès general, de manera que prevalgui l'interès del públic a obtenir-la mitjançant cerques nominals, com pot ser el cas de dades sobre persones amb rellevància a la vida pública. Cal, per tant, fer una valoració cas per cas per tal de determinar quin dret ha de prevaldre en cada situació.

2.3. Aplicació del dret a l'oblit

Des de la sentència Google Spain, tant l'AEPD com els tribunals han resolt molts casos sobre l'aplicació del dret a l'oblit, i s'han anat consolidant alguns criteris, encara que es tracta d'una matèria plena de matisos i en la qual no manquen decisions contradictòries.

Entre altres, es poden destacar les qüestions rellevants següents en l'aplicació d'aquest dret:

1) L'abast territorial del bloqueig. A l'hora de redactar aquest mòdul, és encara una qüestió oberta la de determinar si el cercador està obligat a remoure els resultats a tot el món, i per tant en totes les versions del cercador, o si és suficient que ho faci només en les versions europees (com ara google.es, google.fr, google.it). Hi ha en curs una qüestió prejudicial davant el TJUE, plantejada per l'autoritat de protecció de dades francesa, en què el TJUE s'haurà de pronunciar sobre aquest punt (assumpte C-507/17, Google, *Portée territoriale du déréférencement*). En alguns països l'autoritat de protecció de dades considera que és suficient que el cercador, a més de bloquejar els resultats en els dominis europeus, bloquegi també les cerques en qualsevol altre domini quan són cerques fetes des de la UE, recorrent a la tècnica de la geolocalització i bloqueig geogràfic, per tal d'evitar que des d'Europa es pugui trobar el contingut cercant pel nom en dominis d'altres països, o en el domini .com.

2) La comunicació entre el cercador i la font de la informació. Una altra qüestió debatuda és si el cercador, un cop que ha retirat un enllaç, per exemple un enllaç a una noticia publicada per un diari digital, pot informar d'aquest fet al diari. L'AEPD, en una resolució de setembre del 2016, posteriorment recorreguda i encara pendent de resolució, va considerar que la comunicació a l'editor vulnera el deure de secret que establia l'article 10 de la LOPD de 1999, vigent en aquell moment (resolució R/02232/2016).

3) L'exercici del dret a l'oblit per persones sense vinculació amb la UE. El criteri que s'ha mantingut fins ara és que una persona que no tingui vincles amb la UE, de nacionalitat, residència o d'un altre tipus, no pot fer valer el dret europeu de protecció de dades per a sol·licitar la retirada de resultats en els cercadors.

4) Interès públic de la informació. Com ja s'ha indicat, quan es considera que hi ha un dret prevalent del públic a obtenir la informació de què es tracta, el dret a l'oblit no és procedent. En aquest sentit es poden produir situacions

paradoxals, com ara que quan el mateix interessat del cas Google Spain va demanar la retirada dels enllaços a una entrada de blog que comenta el seu cas, inclosa l'execució de l'immoble i els deutes a la Seguretat Social, l'AEPD va entendre que ara el cas ja és d'interès públic –i de fet el mateix interessat n'havia parlat públicament en diverses entrevistes– i, per tant, la retirada no és procedent (resolució R/02179/2015).

Alguns exemples recents en què s'ha entès que preval l'interès públic són un cas referit a comentaris negatius sobre la conducta professional d'un metge. L'AEPD va estimar el dret a l'oblit, però l'Audiència Nacional va revocar la decisió, considerant que preval l'interès públic perquè els futurs pacients del metge tenen dret a conèixer les experiències i opinions expressades per antics pacients (sentència d'11 de maig del 2017, ECLI: ES:AN:2017:2433).

En un altre cas, l'Audiència Nacional va revocar també la decisió de l'AEPD i va considerar que la informació relativa a les llistes d'unes eleccions municipals és d'interès públic i l'afectat no en pot exigir la retirada en els cercadors (sentència del 19 de juny del 2017, ECLI: ES:AN:2017:2562).

5) Ús de protocols d'exclusió pels editors, per tal d'evitar la indexació de la informació. El Tribunal Suprem, en sentència del 15 d'octubre del 2015 (ECLI: ES:TS:2015:4132) va determinar que un diari ha d'utilitzar protocols d'exclusió (per exemple, el protocol robots.txt) per a assegurar-se que els cercadors no indexaran la informació que contingui dades personals.

6) Integritat de l'hemeroteca digital i ús de cercadors interns. A la mateixa STS del 15 d'octubre del 2015, el Tribunal Suprem va declarar que l'interessat no té dret a exigir que el diari modifiqui el contingut de la seva hemeroteca per a anonimitzar el seu nom en les notícies publicades, o per a substituir-lo per inicials. Va negar també que el diari hagués de bloquejar els resultats de les cerques fetes pel nom de la persona en el cercador intern del web del diari. Aquesta darrera posició, però, ha estat contradita pel Tribunal Constitucional, que en sentència del 4 de juny del 2018 va estimar el recurs d'empara i va anul·lar parcialment la sentència del TS, estimant que l'interessat té dret al bloqueig en les cerques pel seu nom en el cercador intern del diari.

7) Retirada de continguts en plataformes. Mentre que el TJUE va declarar clarament que un cercador és responsable del tractament de les dades indexades, no és tan clar si les plataformes que allotgen continguts pujats pels usuaris s'han de considerar també responsables del tractament de les dades personals que hi ha en aquests continguts. La jurisprudència és encara confusa en aquest punt, però en tot cas l'AEPD estima que un cop que la plataforma ha rebut una notificació de la presència de contingut que vulnera els drets de protecció de dades, té l'obligació de procedir a la retirada del material.

2.4. El dret a l'oblit en el RGPD i en la Llei Orgànica 3/2018

Com indicàvem al principi d'aquest apartat, l'article 17.2 RGPD recull una previsió que vol facilitar la supressió de dades personals a la xarxa. És habitual que la informació que apareix en un lloc web sigui enllaçada des d'altres, o

replicada en altres llocs. L'article 17 estableix els casos en què és procedent el dret a la supressió de les dades amb caràcter general, i afegeix en el seu apartat segon que, quan el responsable del tractament hagi fet públiques les dades i estigui obligat a suprimir-les, ha d'adoptar les mesures raonables per a informar de la sol·licitud de supressió als subsegüents responsables, per tal que suprimeixin «qualsevol enllaç a les dades personals, o qualsevol còpia o rèplica de les dades». Aquesta obligació del responsable del tractament, però, queda supeditada al fet que les mesures siguin raonables «tenint en compte la tecnologia disponible i el cost de la seva aplicació».

La **Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals**, ha afegit una regulació específica sobre el dret a l'oblit. D'una banda, a l'article 93 recull la doctrina emanada del TJUE en la sentència Google Spain en relació amb la supressió de resultats en els cercadors d'internet:

> «1. Tota persona té el dret que els motors de cerca a internet eliminin de les llistes de resultats que s'obtinguessin després d'una recerca efectuada a partir del seu nom els enllaços publicats que continguessin informació relativa a aquesta persona quan fossin inadequats, inexactes, no pertinents, no actualitzats o excessius o haguessin esdevingut com a tals pel transcurs del temps, tenint en compte els fins per als quals es van recollir o tractar, el temps transcorregut i la naturalesa i interès públic de la informació.
>
> De la mateixa manera s'ha de procedir quan les circumstàncies personals que, si s'escau invoqués l'afectat evidenciessin la prevalença dels seus drets sobre el manteniment dels enllaços pel servei de cerca a internet.
>
> Aquest dret subsistirà encara que fos lícita la conservació de la informació publicada al lloc web al qual es dirigís l'enllaç i [aquest web] no procedís esborrar-la de manera prèvia o simultània.
>
> 2. L'exercici del dret a què es refereix aquest article no impedirà l'accés a la informació publicada al lloc web a través de la utilització d'altres criteris de cerca diferents del nom de qui exercís el dret.»

D'altra banda, a l'article 94, titulat *Dret a l'oblit en serveis de xarxes socials i serveis equivalents*, s'estableix el dret a retirar les dades personals que el mateix interessat hagi facilitat per a la seva publicació en xarxes socials. Per a això és suficient la mera sol·licitud de la persona afectada. En relació amb les dades aportades per tercers, es reconeix el dret de l'afectat a la seva supressió quan concorrin els requisits per a l'exercici dels drets de supressió o d'oposició. Aquests requisits, però, no són exigibles quan les dades es refereixin a menors d'edat.

Resum

Les dades personals, qualsevol informació relativa a una persona identificada o identificable, s'han de tractar segons unes normes establertes. No hi ha en el cas de la UE una llibertat total per a tractar les dades, sinó que s'ha de complir amb les disposicions del RGPD i LOPDGDD i en determinats casos amb la normativa específica.

A més de complir amb els principis de protecció de dades, hi ha d'haver una base legal que habiliti el tractament de dades. El responsable del tractament té una sèrie d'obligacions, entre elles la d'informar adequadament l'afectat. A més, ha de portar un registre i tractar les dades de manera adequada, complint amb el principi de responsabilitat proactiva. En el cas de recórrer a un altre subjecte (encarregat del tractament) perquè tracti dades pel seu compte, ha de formalitzar un document on constin tots els extrems d'aquesta relació.

Les autoritats de protecció de dades supervisen el compliment adequat de la normativa. En aquest sentit, el delegat de protecció de dades constitueix un nexe entre les autoritats i les empreses o organitzacions.

L'RT ha de garantir l'exercici dels drets de l'afectat: dret d'accés, rectificació, supressió i oposició. El RGPD també reconeix el dret a la portabilitat de les dades, el dret a no ser objecte de decisions automatitzades sense intervenció humana i a la limitació al tractament.

La transmissió de dades fora de l'EEE constitueix una transferència internacional de dades que està subjecta a unes normes específiques.

El dret a l'oblit ha quedat consagrat des de la sentència del TJUE en el cas Google Spain, que va concloure que els cercadors d'internet són responsables del tractament de les dades personals de totes les informacions que indexen. Com a conseqüència de ser responsables del tractament, els interessats poden sol·licitar al cercador que quan es facin cerques a partir del nom de la persona, no mostri resultats que apuntin a dades personals que no compleixin amb els principis de qualitat o licitud, per exemple, pel fet de tractar-se de dades obsoletes, inexactes, irrellevants o excessives.

Aquest dret també s'ha exercitat enfront dels diaris digitals. El TS ha considerat que no hi ha un dret a anonimitzar els noms de les persones a les hemeroteques digitals. D'altra banda, el TC ha considerat que els interessats poden exigir que es bloquegin resultats també en els cercadors interns d'un diari quan la recerca es fa pel nom de la persona.

El fet de no complir degudament amb la normativa de protecció de dades comporta una infracció normativa que pot suposar sancions econòmiques importants. Així mateix, si com a conseqüència de l'esmentat incompliment s'ocasionen danys a l'afectat, sorgirà una obligació de rescabalar-lo (responsabilitat civil).

Bibliografia

Aparicio Salom, J. (2009). *Estudio sobre la Ley orgánica de protección de datos de carácter personal* (3a. ed.). Navarra: Aranzadi.

Berrocal Lanzarot, A. I. (2017). *Derecho de supresión de datos o derecho al olvido*. Madrid: Editorial Reus.

De Hert, P. J. A.; Papakonstantinou, V. (2014). «The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition». A: *Computer Law & Security Review: the International Journal of Technology Law and Practice* (vol. 30, núm. 6, pàg. 633-642).

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

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

Llácer Matacás, M. R. (2008). «Autodeterminación informativa y valor positivo del silencio. Una lectura crítica del artículo 14 del Reglamento de Protección de Datos Personales». *Derecho privado y Constitución* (núm. 22, pàg. 169-192). ISSN 1133-8768.

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

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

Peguera, M. (2015). «In the Aftermath of Google Spain: How the "Right to Be Forgotten" is Being Shaped in Spain by Courts and the Data Protection Authority». *International Journal of Law and Information Technology*. Vol. 23(4), pàg. 325-347. DOI: 10.1093/ijlit/eav016.

Poullet, Y. (2009, novembre). «Privacy: Conditions for its survival in our I.S.» *31.ª Conferencia Internacional de autoridades de protección de datos y privacidad*. Madrid.

Simón Castellano, P. (2015). *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE*. Barcelona: Editorial Bosch.

Enllaços d'interès

Reglament General de Protecció de Dades:

https://www.aepd.es/normativa/index.html

http://apdcat.gencat.cat/ca/documentacio/RGPD/

http://www.avpd.euskadi.eus/informacion/reglamento-general-de-proteccion-de-datos/s04-5273/es/

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Autoritats de Protecció de Dades:

Agència Espanyola de Protecció de Dades

Autoritat Catalana de Protecció de Dades

Agència Basca de Protecció de Dades

Supervisor Europeu de Protecció de Dades

Altres recursos d'interès:

Comissió Europea

International Association of Privacy Professionals

Future of Privacy Forum

LOPD i Seguretat

Càtedra de privacitat i transformació digital Microsoft-UV

Article 29 working party archives 1997-2016

Normes sobre protecció de dades personals dins i fora de la UE (Comissió europea)

Sobre el mercat únic digital, podeu consultar: Digital Single Market

Pel que fa a les claus de la reforma de la normativa de protecció de dades i les principals característiques del RGPD és molt interessant consultar les Conferències organitzades per l'Autoritat catalana de protecció de dades que aborden les principals qüestions del Reglament 2016/679.