Intimitat i dades personals a Internet

Mònica Vilasau

PID_00242365

Temps mínim previst de lectura i comprensió: **7 hores**

UOC
Universitat Oberta de Catalunya

Índex

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

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

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

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

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

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

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

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

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

Inicialment, aquest dret va quedar delimitat per la Sentència del Tribunal Constitucional alemany de 15 de desembre de 1983, sobre la Llei del cens que va definir el dret a l'autodeterminació informativa com a corol·lari del dret a l'autodeterminació de la persona.

El dret a l'autodeterminació informativa comporta que l'individu pugui decidir bàsicament per si mateix quan i dins de quins límits és procedent revelar situacions referents a la pròpia vida. Segons el Tribunal 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·limitada de les dades referents a la persona.

Sentència del 15 de desembre de 1983

La Sentència del Tribunal Constitucional alemany de 15 de desembre de 1983 pot trobar-se traduïda al castellà en el *Boletín de Jurisprudencia Constitucional*, núm. 33 (1984), pàg. 126 i seg. Es va presentar un recurs contra la Llei del cens de 25 de març de 1982.

Aquest recurs, malgrat reconèixer el dret i el deure de de l'Estat d'obtenir informació, plantejava el temor que la informació pogués ser utilitzada eventualment contra els drets dels ciutadans.

Les normes relatives al tractament de les dades de caràcter personal constitueixen un instrument per a salvaguardar la vida privada del subjecte. No obstant això, a l'hora d'atorgar aquesta protecció, ha de ponderar-se l'existència d'altres drets; especialment la llibertat d'expressió i el dret a comunicar i rebre informació, com també l'accés a la informació generada pel sector públic.

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

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

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

Lectura recomanada

Yves Poullet (2009, novembre)."Privacy: Conditions for its survival in our I.S", 31 Conferència Internacional d'autoritats de protecció de dades i privacitat (pàg. 4). Madrid.http://www.privacyconference2009.org/program/Presentaciones/index-ides-idweb.html).

2. Evolució normativa sobre la protecció de dades

2.1. Marc supranacional

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

En l'àmbit internacional, les primeres iniciatives reguladores van sorgir en el si del Consell d'Europa. En la Resolució de 1968 ja es va subratllar que les "noves tècniques desenvolupades" constitueixen una amenaça als drets i llibertats individuals, especialment al dret de privacitat tutelat en l'article 8 CEDH. En la mesura en què la legislació de la majoria dels estats membres no proporcionava una resposta adequada enfront d'aquestes amenaces i alguns estats estaven planejant revisar la seva legislació sobre aquest tema, es va posar en relleu la necessitat d'aconseguir una major harmonització en la matèria[1].

(1)En l'àmbit nacional cal destacar la Llei aprovada pel Parlament del *land* alemany de Hessen el 1970, i posteriorment països com Suècia, els Estats Units, Alemanya, Dinamarca, Holanda, França, Nova Zelanda o el Canadà van aprovar normativa sobre aquest tema.

Resolució de 1968

Es tracta de la Recommendation 509 (1968), on human rights and modern scientific and technological developments, text adoptat per l'Assemblea el 31 de gener de 1968 (16th Sitting).

Punt 3 de la Recomanació 509

Concretament, en el punt 3 de la Recomanació 509 es declara: "Believing that newly developed techniques such as phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda are a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by Article 8 of the European Convention on Human Rights".

Es va recomanar al Comitè d'Experts en Drets Humans en el si del Consell d'Europa estudiar la qüestió relativa a si l'article 8 CEDH i la legislació dels estats membres protegia adequadament el dret de privacitat respecte de les violacions que es poguessin cometre utilitzant les noves tècniques i mètodes. En cas que la normativa actual no fos suficient, s'aconsellava dur a terme recomanacions per a millorar la protecció del dret a la privacitat.

D'acord amb aquesta invitació, es van aprovar dues resolucions. La Resolució de 1973, que tenia com a objectiu la regulació dels fitxers del sector privat, i la Resolució de 1974, dedicada als fitxers públics. La línia iniciada per les resolucions de 1973 i 1974 es va continuar en el si del Consell d'Europa, on es va gestar el Conveni 108 de 28 de gener de 1981 per a la protecció de les persones pel que fa al tractament automatitzat de dades de caràcter personal. L'objectiu d'aquest Conveni va ser dotar d'un marc general el tractament de dades personals en la mesura que es va arribar a la conclusió que l'article 8 CEDH, que tutela la vida privada, no podia cobrir tots els supòsits de tractament automatitzat de la informació personal ni donar-hi resposta.

Resolució de 1973

Resolution (73) 22 On the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies)

Resolució de 1974

Resolution (74) 29 On the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector (Adopted by the Committee of Ministers on 20 September 1974 at the 236 th meeting of the Ministers' Deputies).

El 1980, l'OCDE va adoptar unes directrius de protecció de dades, amb l'objectiu principal de facilitar les transmissions internacionals de la informació personal.

Lectura recomanada

Sobre les directrius de protecció de dades adoptades per l'OCDE pot consultar-se l'obra de Burkert, que posa en relleu com l'OCDE es va convertir en un fòrum privilegiat d'intercanvi entre Amèrica del Nord i Europa en relació amb la legislació de protecció de dades. Així mateix també recorda el caràcter no vinculant dels Principis OCDE. (H. Burkert, "Privacy-Data Protection: a German/European Perspective", cit., pàg. 51-52).

Posteriorment, cal subratllar l'adopció dels Principis de l'ONU el 1990, que van tractar de fer front a les múltiples qüestions i riscos que la generalització creixent de les TIC plantejava a la societat i concretament al legislador.

Principis de l'ONU de 1990

De Hert i Papakonstantinou assenyalen que lamentablement els Principis de l'ONU de 1990 han estat deixats de banda i això potser ha constituït una oportunitat perduda cap a la consolidació d'uns veritables principis internacionals reguladors de la privacitat informacional. ("The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition", cit., pàg. 634, nota núm. 4).

Conveni 108 de 28 de gener de 1981

Es tracta del Conveni per a la protecció de les persones pel que fa al tractamentautomatitzat de dades de caràcter personal. Aquest text es va aprovar el 28 de gener de 1981 i va entrar en vigor l'1 d'octubre de 1985, després d'aconseguir cinc ratificacions

http://www.coe.int/t/dghl/standardsetting/dataprotection/Global_standard/Conv%20108_es.pdf

http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Després d'un llarg procés de gestació, finalment, en l'àmbit comunitari es va aprovar la Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades[2]. Després d'aquesta norma es va adoptar la Directiva 2002/58/CE del Parlament Europeu i del Consell, de 12 de juliol de 2002, relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques, modificada per la Directiva 2009/136/CE.

[2]Diari Oficial de la Comunitat Europea (DOCE) L 281 (23 de novembre de 1995).

DOCE L 201 (31 de juliol de 2002)

La Directiva 2002/58/CE va derogar la Directiva 97/66/CE, de 15 de desembre de 1997, relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les telecomunicacions.

Directiva 2009/136/CE

La Directiva 2009/136/CE del Parlament Europeu i del Consell de 25 de novembre de 2009 modifica la Directiva 2002/22/CE relativa al servei universal i els drets dels usuaris en relació amb les xarxes i els serveis de comunicacions electròniques, la Directiva 2002/58/CE relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques i el Reglament (CE) núm. 2006/2004 sobre la cooperació en matèria de protecció dels consumidors, Diari Oficial de la Unió Euro-

pea, (DOUE) L 337 (18 de desembre de 2009). Aquesta Directiva, al seu torn, està essent objecte de reforma, per alinear-la adequadament amb l'agenda digital. Es va iniciar un procés de consulta pública que va finalitzar el 5 de juliol de 2016. Sobre aquest tema pot consultar-se:

https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive

També ha de tenir-se en compte la Directiva 2006/24/CE del Parlament Europeu i del Consell, de 15 de març de 2006, sobre la conservació de dades generades o tractades en relació amb la prestació de serveis de comunicacions electròniques d'accés públic o de xarxes públiques de comunicacions, i per la qual es modifica la Directiva 2002/58/CE[3]. Aquesta Directiva va ser declarada nul·la pel TJUE com a conseqüència del cas *Digital Rights Ireland*.

[(3)]DOCE L 105 (13 d'abril de 2006)

Cas *Digital Rights Ireland*

Es tracta de la STJUE (Gran Sala), de 8 d'abril de 2014, Assumptes acumulats C-293/12 i C-594/12. Digital Rights Ireland Ltd (C-293/12) contra Minister for Communications, Marine and Natural Resources i altres i Kärntner Landesregierung (C-594/12) i altres. Peticions de decisió prejudicial plantejades per la High Court of Ireland (Irlanda) i Verfassungsgerichtshof (Àustria).

Finalment, en l'àmbit de la UE, ha de destacar-se la Carta dels drets fonamentals de la Unió Europea, de 7 de desembre de 2000, en què els articles 7 i 8 es dediquen, respectivament, al respecte a la vida privada i familiar i a la protecció de dades de caràcter personal.

Carta dels drets fonamentals

Pot consultar-se la Carta dels drets fonamentals de la Unió Europea en la versió consolidada: DOUE, C 83 (30 de març de 2010).

Si la Convenció del Consell d'Europa de 1981 i la Directiva 95/46 van significar una resposta al tractament de dades des d'una perspectiva europea, en els països de l'APEC (*Àsia Pacific Economic Cooperation*) també es va donar una resposta, mitjançant l'adopció al seu torn d'uns principis el 2005. Es tracta d'uns principis que són aplicables, entre altres, a països tan diversos com els Estats Units, el Vietnam, el Canadà, la Xina, el Japó, Rússia o Xile.

APEC

L'APEC està integrada per 21 països. Pot consultar-se la relació completa de països que integren aquesta organització a: http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx.

APEC Privacy Framework

El novembre del 2004, els ministres de les economies que integren l'APEC http://www.apec.org/, reunits a Santiago de Xile van adoptar l'"APEC Privacy Framework", que va ser desenvolupada durant els anys 2003 i 2004 pel Grup de Comerç Electrònic de l'APEC, subgrup sobre la privacitat. El marc de l'APEC consistia originalment en un conjunt de nou principis (que integraven la tercera part del document), precedits per un prefaci, un preàmbul (part I) i una segona part dedicada a l'àmbit d'aplicació. La quarta part del marc de privacitat de l'APEC es dedicava a la implementació dels principis, si bé només es feia referència a la implementació en l'àmbit nacional (part A). El setembre de 2005 es va afegir una segona part B dedicada a la implementació en l'àmbit internacional, i es completaven així els principis el 2005.

L'adopció de tots els textos referits va constituir sens dubte una fita important en la regulació de les noves tecnologies i la consagració del dret a la protecció de dades. No obstant això, en la mesura que les TIC evolucionen constantment, en part es pot afirmar que algunes d'aquestes normes ja van néixer massa tard. Concretament se'n constata la limitació per a fer front a una realitat que va evolucionant, generant i transmetent contínuament dades personals. La digitalització i transmissió de les dades personals és un fenomen imparable en la societat actual. La majoria dels textos analitzats no podien preveure la revolució que va constituir Internet. Aquest fenomen comporta que hagin de repensar-se i redissenyar-se les normes que regulen el tractament de la informació personal.

Un bon exemple d'aquesta urgència d'aconseguir uns principis universals que donin resposta a aquests nous reptes el constitueix l'adopció de la Resolució de Madrid, adoptada el 2009. Es tracta dels Estàndards Internacionals sobre Protecció de Dades Personals i Privacitat. Resolució de Madrid, que van ser aprovats en la 31a. Conferència Internacional d'Autoritats de Protecció de Dades. El text aprovat pot trobar-se a: http://www.agpd.es/portalwebAGPD/internacional/Estandares_Internacionales/contenido-ides-idphp.php.

Quant a la revisió dels textos ja adoptats per a donar resposta als nous reptes, s'ha de fer referència a tres processos diferents d'actualització que van començar al voltant del 2010. En primer lloc, l'OCDE va modificar els Principis de 1980, procés que va culminar el 2013 amb l'aprovació d'uns nous principis.

Al Consell d'Europa també el 2010 es van iniciar els treballs de revisió del Conveni 108. El Comitè Consultiu creat per a aquest Conveni (T-PD)[4] va decidir, en la seva 25a. trobada plenària el setembre de 2009, establir com a prioritat la preparació d'esmenes al text de 1981, procés de reforma que encara no ha acabat.

Finalment, en el si de la UE, el maig de 2009 la Comissió Europea va llançar un procés de reforma de la Directiva 95/46. El gener de 2012, la Comissió va concretar aquesta reforma amb la presentació de dos textos normatius, una proposta de reglament i una proposta de directiva, que després d'un llarg procés d'elaboració van ser aprovades l'abril de 2016. Es tracta del Reglament 2016/679[5] 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, i de la Directiva 2016/680[6] relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les autoritats competents per a finalitats de prevenció, investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals, i a la lliure circulació d'aquestes dades i per la qual es deroga la Decisió marc 2008/977/JAI del Consell.

(4)Capítol V del Conveni 108, arts. 18-20

Enllaç d'interès

Quant a l'estat actual de la reforma del Conveni 108, podeu consultar l'adreça webs següent:http://www.coe.int/t/dghl/standardsetting/dataprotection/Cahdata_en.asp

(5)El Reglament 2016/679 (RGPD) es troba publicat al DOUE de 4 de maig de 2016, L 119/1.

(6)La Directiva 2016/680 es troba publicada al DOUE de 4 de maig de 2016, L 119/89.

Reforma de la Directiva 95/46 i adopció del Reglament 2016/679

El punt de partida de la reforma de la Directiva 95/46 i de l'adopció del Reglament 2016/679 el constitueix el reconeixement del dret a la protecció de dades a la CDFUE (art. 8), així com en el Tractat de Lisboa. La base jurídica de les normes de protecció de dades en el marc de les activitats regulades pel dret de la UE es recull en l'article 16 del Tractat de Funcionament de la Unió Europea (versió consolidada del Tractat de funcionament de la Unió Europea, DOUE, C 115/47, de 9.5.2008).

També han d'esmentar-se els passos que han fet els Estats Units sota la presidència d'Obama. El febrer de 2012, la Casa Blanca va publicar un llibre blanc relatiu a la privacitat de les dades del consumidor en un món connectat. Es tractava de la proposta d'un marc per a protegir la privacitat i promoure la innovació en l'economia global digital. Després de més de dos anys de consultes entre els sectors implicats, el febrer de 2015 la Casa Blanca va donar a conèixer un esborrany de text sobre la Llei relativa a la privacitat del consumidor, es tracta de la *Consumer Privacy Bill of Rights Act* (CPBR). Constitueix una norma d'àmbit federal relativa al tractament de dades en el sector privat, la finalitat de la qual és configurar el marc regulador de la privacitat així com la seva aplicació en l'esfera comercial. Un altre objectiu és el de promoure la implementació d'aquesta protecció mitjançant codis de conducta desenvolupats pels sectors implicats.

2.2. El marc legal aplicable a l'Estat espanyol

2.2.1. Marc normatiu

L'article 18.4 CE estableix que

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

Partint d'aquest precepte i en funció de la matèria de què es tracti, hi ha diferents blocs normatius que s'apliquen de manera més o menys immediata. A més, com a resultat de la distribució de competències entre l'Estat i les comunitats autònomes, també cal tenir en compte les normes dictades en cadascuna d'aquestes instàncies.

L'article 18.4 CE es va desenvolupar mitjançant la Llei orgànica 5/1992, de 29 d'octubre, de regulació del tractament automatitzat de dades de caràcter personal (LORTAD[7]). Aquesta Llei va ser derogada per la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD). Així doncs, un primer bloc normatiu per raó de la matèria està integrat principalment per la LOPD, que constitueix el text bàsic i de caràcter general sobre la protecció de dades, juntament amb el reglament que la desenvolupa, el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (RLOPD).

[7] Llei orgànica 5/1992, de 29 d'octubre, de regulació del tractament automàtic de dades de caràcter personal.

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

Normes específiques

Entre d'altres, vegeu: Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i dels drets i obligacions en matèria d'informació i documentació clínica; Llei 14/2007, de 3 de juliol, de recerca biomèdica; Llei orgànica 10/2007, de 8 d'octubre, reguladora de la base de dades policial sobre identificadors obtinguts a partir de l'ADN; Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.

Un segon bloc normatiu estaria integrat per les disposicions relatives al comerç i a l'administració electrònica. Així mateix, dins del context d'Internet i també en matèria de protecció de dades, cal fer referència als elements d'autoregulació que sorgeixen. Es tracta de mecanismes d'autocontrol que normalment es donaran en el sector privat, però que no són exclusius d'aquest àmbit. Constitueixen un exemple d'aquesta activitat els denominats *codis tipus*, codis[8] de conducta que poden acordar un grup d'empreses o les administracions públiques a fi d'establir una sèrie de regles, condicions d'organització, règim de funcionament, procediments aplicables, normes de seguretat, polítiques en el tractament de les dades personals, etc.

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

Disposicions relatives al comerç i a l'administració electrònica

Entre d'altres, vegeu: Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (LSSI); Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic; Llei 56/2007, de 28 de desembre, de mesures d'impuls de la societat de la informació; Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern; Llei 9/2014, de 9 de maig, General de Telecomunicacions; Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques i Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic.

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

Disposicions de caràcter general

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

Dins del marc regulador de la protecció de dades cal tenir en compte la presència tant de normes estatals com de normes autonòmiques. L'Agència Espanyola de Protecció de Dades és l'autoritat de control competent per a salvaguardar el respecte del dret fonamental a la protecció de dades pel que fa als tractaments de dades efectuats principalment pel sector privat i pel sector públic en els casos que no quedin sota el control d'una autoritat autonòmica. Catalunya i el País Basc, dins el marc competencial que els atorguen la CE i els seus respectius Estatuts d'Autonomia, han dictat també les seves pròpies normes.

L'article 41 de la LOPD permet que determinades funcions de l'Agència Espanyola de Protecció de Dades (AEPD), quan afectin fitxers de dades de caràcter personal creats o gestionats per les comunitats autònomes i per l'administració local, siguin exercides pels òrgans corresponents de cada comunitat, que tenen la consideració d'autoritats de control. Algunes comunitats autònomes han creat les respectives agències de protecció de dades i la corresponent normativa que les desenvolupa.

La primera autoritat de control autonòmica va ser la de la comunitat de Madrid, creada mitjançant la Llei 13/1995, de 21 d'abril, de regulació de l'ús de la informàtica en el tractament de dades personals per la Comunitat de Madrid, i que va ser suprimida amb efectes a partir de gener de 2013. En el cas de la comunitat autònoma de Catalunya, l'article 31 del seu Estatut d'autonomia[9] reconeix el dret a la protecció de dades personals, i l'article 156 estableix les competències de la Generalitat en matèria de protecció de dades de caràcter personal. Abans ja s'havia creat l'Agència Catalana de Protecció de Dades mitjançant la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades, derogada per la Llei 32/2010, que va deixar pas a l'Autoritat Catalana de Protecció de Dades[10].

L'última autoritat de control autonòmica creada va ser la basca, mitjançant la Llei 2/2004, de 25 de febrer, de fitxers de dades de caràcter personal de titularitat pública i de creació de l'Agència Basca de Protecció de Dades.

Les agències autonòmiques tenen principalment encomanada la funció de vetllar pels fitxers de caràcter públic dels seus àmbits territorials i també poden tenir competències respecte determinats fitxers privats. Les seves respectives lleis determinen el seu àmbit d'actuació.

(9)Llei orgànica 6/2006, de 19 de juliol, de reforma de l'Estatut d'autonomia de Catalunya, publicada pel Decret 306/2006, de 20 de juliol, pel qual es dóna publicitat a la Llei orgànica 6/2006, de 19 de juliol, de reforma de l'Estatut d'autonomia de Catalunya.

(10)Es tracta de la Llei 32/2010, d'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades (DOGC núm. 5731, de 8.10.2010).

APDCM

La Llei de mesures fiscals i administratives per a l'any 2013 de la comunitat de Madrid va declarar la supressió de l'Agència de Protecció de Dades de la comunitat de Madrid (APDCM) i la derogació de la Llei 8/2001, de 13 de juliol.

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

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

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

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

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

D'altra banda, pel que fa al contingut, és a dir, les facultats que aquests preceptes atorguen al titular del dret, l'article 18.1 CE confereix a aquest titular el poder jurídic d'imposar a tercers el deure abstenir-se de tota intromissió en l'esfera íntima de la persona i la prohibició de fer ús del que mitjançant una intromissió hagi estat conegut. En canvi, el dret a la protecció de dades atribueix

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

En definitiva, el contingut del dret fonamental a la protecció de dades consisteix en un poder de disposició i de control sobre les dades personals que faculta a la persona per decidir quines dades proporciona a un tercer, sigui l'Estat o un particular, o quines pot obtenir aquest tercer. Aquest dret també permet a l'individu saber qui posseeix aquestes dades personals, saberamb quina finalitat les posseeix i oposar-se a aquesta possessió o ús. Aquests poders de disposició i control sobre les dades personals, que constitueixen part del contingut del dret fonamental a la protecció de dades, es concreten jurídicament en la facultat de consentir la recollida, l'obtenció i l'accés a les dades personals: el seu emmagatzematge i tractament posteriors, i també el seu ús possible per part d'un tercer, sigui l'Estat o un particular. I aquest dret a consentir el coneixement i el tractament, informàtic o no, de les dades personals, requereix, com a complements indispensables, d'una banda, la facultat de saber en tot moment qui disposa d'aquestes dades personals i a quin ús les sotmet i, d'altra banda, el fet de poder oposar-se a aquesta possessió i aquests usos (STC 292/2000, FJ 7).

3. El Reglament general de protecció de dades (Reglament 2016/679): aspectes clau

El Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 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, en endavant RGPD) es va publicar en el DOUE de 4 de maig, si bé no serà aplicable fins al 25 de maig de 2018.

Aquest text constitueix el marc general de regulació del tractament de dades de caràcter personal. Juntament amb aquesta norma hi ha altres textos que regulen el tractament de la informació. Entre d'altres cal destacar: l'àmbit de les comunicacions electròniques (Directiva 2009/136/CE, que està sent objecte de reforma); el tractament per part de les institucions i organismes de la UE (Reglament 45/2001); el processament per a fins de prevenció, investigació, detecció o enjudiciament d'infraccions penals o execució de sancions penals (Directiva 2016/680) o bé el processament de les dades del registre de noms de passatgers (PNR), regulats per la Directiva 2016/681.

Reglament (CE) núm. 45/2001

El Reglament (CE) núm. 45/2001 del Parlament Europeu i del Consell, de 18 de desembre de 2000, regula la protecció de les persones físiques pel que fa al tractament de dades personals per les institucions i els organismes comunitaris i a la lliure circulació d'aquestes dades. Aquest Reglament estableix el marc legal de protecció de dades en les institucions europees i disposa la creació del supervisor europeu de protecció de dades, autoritat supervisora independent d'àmbit comunitari. El Reglament general de protecció de dades manté la vigència del Reglament 45/2001 (vegeu. art. 2.3 RGPD) si bé, com estableix aquest precepte, s'ha d'adaptar als principis i normes d'aquest Reglament de conformitat amb el seu article 98.

Directiva (UE) 2016/681

La Directiva (UE) 2016/681 del Parlament Europeu i del Consell, de 27 d'abril de 2016, regula la utilització de dades del registre de noms dels passatgers (PNR) per a la prevenció, detecció, investigació i enjudiciament dels delictes de terrorisme i de la delinqüència greu.

3.1. Introducció, objectius i característiques generals

Els inicis de la reforma es remunten al 2009 i 2010, amb l'obertura de consultes sobre la seva conveniència. El gener de 2012, la Comissió va presentar la Proposta de reforma del marc regulador de la protecció de dades, que ja incloïa una proposta de reglament i una de directiva. L'aprovació del Reglament 2016/679 i de la Directiva 2016/680 comporta que la pràctica totalitat de processament de dades a la UE queda coberta sota una normativa reguladora. De fet, no hi haurà tractament de dades que no estigui sota una regulació o una altra.

3.1.1. Les raons d'una reforma

La reforma de la DPD i la proposta d'un Reglament que la substitueixi obeeix a diferents factors.

Enllaç d'interès

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

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

En primer lloc, els canvis tecnològics, singularment l'ús generalitzat i constant d'Internet. Si bé en el moment d'adoptar-se la DPD ja existia Internet, l'ús que en aquell moment es feia de la Xarxa encara era incipient.

En segon lloc, cada vegada era més acusada una divergència normativa entre les legislacions dels estats membres. La diferència en la transposició de la Directiva pels diferents estats també comporta, a més, un sobrecost per a les empreses en la mesura que ha d'adaptar-se a les diferents legislacions. Aquesta discrepància era rellevant, un exemple paradigmàtic el constitueix el règim sancionador, que en alguns països és pràcticament inexistent mentre que en altres comporta la imposició d'importants sancions econòmiques.

Aquestes divergències comporten dificultats per a les APD (autoritats de protecció de dades) quan han de donar resposta a conflictes que afecten diferents estats i diferents legislacions. De vegades no resulta fàcil determinar quina llei és aplicable o quina autoritat ha d'intervenir.

La reforma empresa s'incardina en l'agenda digital presentada per la Comissió. És a dir, es tracta d'afermar la confiança en l'entorn digital, a fi de potenciar i fer créixer el comerç electrònic. La finalitat és la de facilitar i buscar un increment de la competitivitat de les empreses europees respecte d'altres entorns. Els objectius són els de garantir la seguretat jurídica, simplificar la regulació, eliminar càrregues burocràtiques i establir regles clares per a les transferències internacionals de dades (si bé aquest objectiu dista molt d'haver estat aconseguit).

3.1.2. Les característiques principals de la nova regulació

Quant a les característiques del RGPD, en primer lloc ha de subratllar-se la importància que es tracti d'un reglament, la qual cosa comporta una novetat en la protecció dels drets fonamentals a la UE. No obstant això, una crítica que cal fer a aquesta norma és que és excessivament reglamentista[11].

(11)El Reglament preveu l'existència d'actes delegats i actes executius, i també disposa les remissions a la regulació per part dels estats en determinats preceptes.

No obstant això, tot i tractar-se d'un reglament i de la seva vocació uniformadora, han quedat molts sectors fora[12].

(12)Per exemple, el sector regulat per la Directiva 2016/680 o el tractament de dades per part de les institucions, òrgans i organismes de la UE.

Es procura reforçar el paper de les APD, i de fet la regulació d'aquestes i la seva relació amb la Comissió i la cerca d'un equilibri entre elles va ser un dels esculls principals en la negociació del Reglament.

S'estableix un règim sancionador que preveu la imposició d'importants sancions econòmiques.

3.2. Àmbit d'aplicació

L'article 1 RGPD disposa que:

> "1. Aquest Reglament estableix 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.
>
> 2. Aquest Reglament protegeix els drets i llibertats fonamentals de les persones físiques i, en particular, el seu dret a la protecció de les dades personals.
>
> 3. La lliure circulació de les dades personals a la Unió no es pot restringir ni prohibir per motius relacionats amb la protecció de les persones físiques pel que fa al tractament de dades personals."

3.2.1. Àmbit material d'aplicació

Supòsits als que resulta aplicable el Reglament 2016/679

> **Art. 2.1.**
>
> "Aquest Reglament s'aplica al tractament totalment o parcialment automatitzat de dades personals, així com al tractament no automatitzat de dades personals contingudes o destinades a ser incloses en un fitxer."

1) Persones físiques. La norma fa referència a dades de persones físiques identificables, per tant queden excloses les persones jurídiques. Com recorda el considerant 14 RGPD:

> "Aquest Reglament no regula el tractament de dades personals relatives a persones jurídiques i en particular a empreses constituïdes com a persones jurídiques, inclòs el nom i la forma de la persona jurídica i les seves dades de contacte."

El RGPD no contempla les dades relatives a les persones mortes. Referent a això, en el cas de l'ordenament jurídic espanyol, resulta aplicable l'art. 2.4 RLOPD.

2) Dada personal. El RGPD fa referència a les dades personals, i es considera com a tal

> "tota informació sobre una persona física identificada o identificable ("l'interessat"); es considera persona física identificable tota persona la identitat de la qual pugui determinar-se, directament o indirectament, en particular 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" (art. 4.1).

Dades genètiques i dades biomètriques

Quant a què ha d'entendre's per *dades genètiques*, vegeu l'article 4 (13) RGPD. Quant a dades biomètriques, l'article 4 (14) RGPD.

Quant a les denominades *dades sensibles* (categories especials de dades, art. 9 RGPD), es manté, en termes generals, la fórmula de la DPD.

En configurar les dades sensibles, aspecte que serà analitzat amb més detenciment en tractar del consentiment del subjecte afectat, hi ha dues aproximacions possibles. Una de més dinàmica, que tindria en compte qualsevol tipus de dada que pogués revelar informació sensible. En conseqüència podria incloure's, per exemple, les dades relatives a hàbits alimentaris o fins i tot el cognom. I una concepció més estàtica que parteix d'una llista de dades que es qualifiquen com a *sensibles*. Aquesta última configuració és la que adopta l'article 9 RGPD i que és, en termes generals, la que es recull en l'art. 8 DPD.

Si bé el terme *revelar*, adoptat per l'article 9.1 RGPD podria donar a entendre que se segueix una perspectiva dinàmica, aquesta no és la interpretació que s'ha donat al precepte en qüestió. Les dades es distingeixen entre sensibles i no sensibles segons la seva naturalesa i no segons el seu ús potencial.

3) Tipus de tractament. S'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. Es manté per tant una situació similar a la de la DPD.

Considerant (15) RGPD

"A fi d'evitar que hi hagi un greu risc d'elusió, la protecció de les persones físiques ha de ser tecnològicament neutra i no ha de dependre de les tècniques utilitzades. La protecció de les persones físiques ha d'aplicar-se al tractament automatitzat de dades personals, així com al seu tractament manual, quan les dades personals figurin en un fitxer o estiguin destinades a ser-hi incloses. Els fitxers o conjunts de fitxers, així com les seves portades, que no estiguin estructurats conformement a criteris específics, no han d'entrar en l'àmbit d'aplicació d'aquest Reglament."

Supòsits als quals no resulta aplicable el RGPD

Segons l'article 2.2 RGPD, "Aquest Reglament no s'aplica al tractament de dades personals":

a) en l'exercici d'una activitat no compresa en l'àmbit d'aplicació del dret de la Unió;

Considerant (16) RGPD

"Aquest Reglament no s'aplica a qüestions de protecció dels drets i les llibertats fonamentals o la lliure circulació de dades personals relacionades amb activitats excloses de l'àmbit del dret de la Unió, com les activitats relatives a la seguretat nacional. Tampoc no s'aplica al tractament de dades de caràcter personal pels estats membres en l'exercici de les activitats relacionades amb la política exterior i de seguretat comuna de la Unió".

b) per part dels estats membres quan duguin a terme activitats compreses en l'àmbit d'aplicació del capítol 2 del títol V del TUE. Es tracta dels supòsits de política exterior i de seguretat comuna.

c) efectuat per una persona física en l'exercici d'activitats exclusivament personals o domèstiques.

Sobre aquest tema és fonamental tenir en compte el considerant (18):

"Aquest Reglament no s'aplica al tractament de dades de caràcter personal per una persona física en el curs d'una activitat exclusivament personal o domèstica i, per tant, sense cap connexió amb una activitat professional o comercial. Entre les activitats personals o domèstiques cal incloure la correspondència i la gestió d'un repertori d'adreces, o l'activitat en les xarxes socials i l'activitat en línia duta a terme 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 tractar dades personals relacionades amb aquestes activitats personals o domèstiques".

Això té una sèrie de conseqüències respecte als usuaris de les xarxes socials, perquè quan es tracta d'un individu (particular) que les utilitza per a relacionar-se amb els seus 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.

d) Per part de les autoritats competents amb finalitats de prevenció, investigació, detecció o enjudiciament d'infraccions penals, o d'execució de sancions penals, inclosa la de protecció enfront d'amenaces a la seguretat pública i la seva prevenció[13].

[13] Vegeu sobre aquest tema els considerants 19 I, 19.II i 20.

A més, l'article 2.3 RGPD disposa que

"El Reglament (CE) núm. 45/2001 és aplicable al tractament de dades de caràcter personal per part de les institucions, òrgans i organismes de la Unió. El Reglament (CE) núm. 45/2001 i altres actes jurídics de la Unió aplicables a aquest tractament de dades de caràcter personal s'han d'adaptar als principis i normes d'aquest Reglament de conformitat amb el seu article 98."

Considerant (17) RGPD

"El Reglament (CE) núm. 45/2001 del Parlament Europeu i del Consell (2) s'aplica al tractament de dades de caràcter personal per les institucions, òrgans i organismes de la Unió. El Reglament (CE) núm. 45/2001 i altres actes jurídics de la Unió aplicables a aquest tractament de dades de caràcter personal han d'adaptar-se als principis i normes establerts en aquest Reglament i aplicar-se segons aquest. A fi d'establir un marc sòlid i coherent en matèria de protecció de dades a la Unió, una vegada adoptat aquest Reglament, han d'introduir-se les adaptacions necessàries del Reglament (CE) núm. 45/2001, amb la finalitat de poder aplicar-se al mateix temps que aquest Reglament."

Finalment, segons determina l'article 2.4 RGPD[14],

[14] Vegeu sobre aquest tema el considerant 21.

"Aquest Reglament s'entén sense perjudici de l'aplicació de la Directiva 2000/31/CE, en particular les seves normes relatives a la responsabilitat dels prestadors de serveis intermediaris establertes en els articles 12 a 15".

3.2.2. Àmbit territorial d'aplicació

Segons disposa l'article 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 en la Unió, independentment que el tractament tingui lloc en la Unió o no".

Per tant, el criteri que ara permet determinar l'aplicació de la norma europea és el criteri d'un establiment a la UE, amb independència del lloc on es duu a terme el tractament.

Però el RGPD va més enllà i disposa l'aplicació del mateix fins i tot quan el responsable del tractament (RT) no estigui establert a la Unió.

Segons preveu l'article 3.2. RGPD:

> "Aquest Reglament s'aplica al tractament de dades personals d'interessats que resideixin a la Unió per part d'un responsable o encarregat no establert a la Unió, quan les activitats de tractament estiguin relacionades amb:
>
> **a)** l'oferta de béns o serveis a aquests interessats a la Unió, independentment de si a aquests se'ls requereix el seu pagament[15].
>
> La finalitat d'aquesta disposició és que les persones físiques no es vegin privades de la protecció a la qual tenen dret en virtut d'aquest Reglament.
>
> Per a determinar si aquest responsable o encarregat ofereix béns o serveis a interessats que resideixin a la Unió, ha de determinar-se si és evident que el responsable o l'encarregat projecta oferir serveis a interessats en un o més dels estats membres de la Unió. Per a determinar aquest extrem, es tenen en compte aspectes com la llengua de la pàgina web, la moneda utilitzada en el pagament o bé on es produeix el lliurament dels béns.
>
> b) el control del seu comportament, en la mesura en què aquest tingui lloc a la Unió.
>
> 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, analitza o prediuen les preferències personals, comportaments i actituds dels afectats[16]."

(15) Considerant 23

(16) Considerant 24

S'ha de tenir en compte que, en aquests casos (art. 3.2 RGPD), és necessari designar un representant a la UE (art. 27.1 i 27.2 RGPD).

Finalment, segons disposa l'article 3.3, el RGPD resulta aplicable quan això es deriva de les normes de dret internacional públic:

> "Aquest Reglament s'aplica al tractament de dades personals per part d'un responsable que no estigui establert a la Unió sinó en un lloc en què el dret dels estats membres sigui aplicable en virtut del dret internacional públic".

3.2.3. Entrada en vigor del RGPD

El RGPD es va publicar en el DOUE de 4 maig 2016 i va entrar en vigor el 25 de maig de 2016. No obstant això, fins el 25 de maig de 2018 no serà plenament aplicable. Entretant resulta plenament aplicable la LOPD i el RLOPD.

A partir del 25 de maig de 2018, la LOPD i el RLOPD podran seguir essent aplicables sempre que no siguin contraris a la norma de la UE. En relació amb els aspectes regulats per la LOPD i també regulats pel RGPD, la LOPD queda desplaçada. Això és així sempre que els estats no tinguin una habilitació per a regular un determinat aspecte, habilitació basada en el mateix RGPD.

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

L'article 5 RGPD, sota la rúbrica "**Principis relatius al tractament**", recull quins són els principis de protecció de dades, posant un nom a cadascun.

D'entrada cal assenyalar que no hi ha grans canvis dels principis recollits en el RGPD respecte dels admesos en la DPD i en la mateixa LOPD. L'única novetat com a tal la representa el principi de responsabilitat proactiva (art. 5.2 RGPD).

Es tracta dels principis següents.

Primer, les dades personals s'han de tractar de manera lícita, lleial i transparent en relació amb l'interessat ("licitud, lleialtat i transparència", art. 5.1.a) RGPD).

Aquests tres principis estan molt interconnectats. El principi de lleialtat i el de transparència estan molt lligats, de manera que ha d'informar-se de què es farà amb les dades. De fet, el principi de transparència està lligat a l'exercici de tots els drets.

Com s'ha indicat, aquests principis no representen una gran innovació ni se separen de les previsions de la DPD ni de la LOPD. De fet, l'article 4 LOPD, en recollir el que es coneixia com a *principi de qualitat de les dades*, prohibeix la recollida de les dades per mitjans fraudulents, deslleials o il·lícits.

L'article 4.7 LOPD disposa que "Es prohibeix la recollida de dades per mitjans fraudulents, deslleials o il·lícits".

El principi de transparència tampoc no és nou, ja que també està recollit en la LOPD, si bé en aquesta última no es formula com un principi, sinó com una obligació del responsable del tractament (art. 5 LOPD). Ara el RGPD tracta la transparència com un principi, i més endavant, en el seu articulat, com un dret. A més, cal recordar que segons el TC la transparència representa un pressupost de l'exercici dels altres drets.

Quant al principi de licitud, aquest es troba més desenvolupat en l'article 6 RGPD. La legislació espanyola, en recollir aquest principi, ho va fer sota la rúbrica de *principi del consentiment*, en l'article 6 LOPD. Tanmateix en aquest article, a més del consentiment es regulen els altres supòsits que habiliten el tractament de les dades de caràcter personal (DCP en endavant).

Habilitació

En el marc de la LOPD, els articles 11 i 21 LOPD preveuen supòsits concrets d'habilitació. L'article 11 LOPD respecte de la cessió de dades, i l'article 21 LOPD respecte de habilitació específica per a un supòsit concret (comunicació de dades entre administracions). En canvi, el RGPD no fa cap referència a les comunicacions de dades i ni tan sols proporciona la definició d'aquest terme. La DPD tampoc no proporciona definició del terme *comunicació* com sí fa en canvi l'article 3.i) LOPD. Per contra, el RGPD sí proporciona una definició de *destinatari d'una comunicació* (art. 4.9 RGPD) i ha de subratllar-se que s'entén per *destinatari* tant la persona física com un servei.

Quant als supòsits d'habilitació, el RGPD adopta una sistemàtica molt semblant a la DPD i exposa quins són els mecanismes d'habilitacions. Tampoc no hi ha novetats rellevants, i seran analitzades en l'epígraf següent.

L'article 6 RGPD, en regular les habilitacions, parteix del mateix punt que ho fa la DPD.

Segon, les dades personals s'han de recollir amb finalitats determinades, explícites i legítimes, i no es poden tractar 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 de recerca científica i històrica o finalitats estadístiques no es considera incompatible amb les finalitats inicials ("limitació de la finalitat", art. 5.1.b) RGPD).

Article 4.2 LOPD

"Les dades de caràcter personal objecte de tractament no poden usar-se per a finalitats incompatibles amb aquelles per a les quals les dades hagin estat recollides. No es considera incompatible el tractament posterior d'aquestes amb finalitats històriques, estadístiques o científiques"

Quant al principi de finalitat: l'article 4 LOPD diu que no poden usar-se per a *finalitats* incompatibles, mentre que l'article 5.1.b) RGPD fa referència al fet que no poden ser tractades ulteriorment de "*manera* incompatible", la qual cosa és una mica diferent.

Una altra novetat que representa l'article 5.1.b) és fer referència també al "tractament ulterior de les dades personals amb finalitats d'arxiu en interès públic", la qual cosa no preveia ni l'article 4.2 LOPD ni l'article 6.1.b DPD. L'article 4.2 LOPD disposa que "No es considera incompatible el tractament posterior d'aquestes dades amb finalitats històriques, estadístiques o científiques", però no fa referència a la finalitat d'arxiu.

La qüestió és determinar què ha d'entendre's per *arxiu en interès públic*. Es tracta solament d'un arxiu públic o també pot comprendre un arxiu privat però d'interès públic?

Sembla clar que queden compresos els arxius que tenen cabuda dins de la Llei de patrimoni nacional i dins de les Lleis d'arxius de les diferents comunitats autònomes en cas que n'hi hagi. Però sembla que també haurien d'incloure's els arxius privats d'interès públic.

El precepte en qüestió es remet a l'article 89 RGPD (Garanties i excepcions aplicables al tractament amb finalitats d'arxiu en interès públic, finalitats de recerca científica o històrica o finalitats estadístiques), en regular l'ús de les dades. Es disposa que cal l'adopció de mesures adequades.

En qualsevol cas, l'aspecte més nou respecte de l'article 5.1.b és que es relativitza la "incompatibilitat" respecte de les finalitats.

Efectivament, l'article 6.4 RGPD admet en determinats supòsits destinar les dades a una finalitat diferent. En aquest cas és el RT qui ha de valorar si l'ús de les dades per a una altra finalitat és compatible o no.

Com ha de valorar el RT si el canvi de finalitat és possible o no? El paràmetre i el criteri el proporciona l'article 6.4 RGPD. Sens dubte això implica obrir la porta a un terreny que generarà dubtes al RT i també a les APD.

Quant al canvi de finalitat, també s'ha detenir en compte l'article 23.2 RGPD (relatiu a les limitacions).

> Tercer, les dades personals han de ser adequades, pertinents i limitades al que sigui necessari en relació amb les finalitats per a les quals són tractades ("minimització de dades", art. 5.1.c) RGPD).

El principi de minimització tampoc no representa en rigor un nou principi. La LOPD ja estableix que les dades poden ser tractades quan siguin adequades, pertinents i no excessives en relació amb la finalitat. Això és, el tractament ha de ser proporcional a la finalitat.

Això comporta que, en dur a terme un tractament, en primer lloc hagi de valorar-se si efectivament cal tractar DCP. En cas que hagin de tractar-se dades: que aquest tractament sigui l'imprescindible per a la finalitat prevista. En aquest punt rellevant, un concepte lligat a la minimització és el de seudonimització.

Segons es determina en l'article 4. (5) RGPD, s'entén per *seudonimització*: el tractament de dades personals de manera que ja no puguin atribuir-se a un interessat sense utilitzar informació addicional, sempre que aquesta informació addicional figuri per separat i estigui subjecta a mesures tècniques i organitzatives destinades a garantir que les dades personals no s'atribueixin a una persona física identificada o identificable.

El concepte de *seudonimització* és un concepte nou, un mecanisme que permet tractar dades que s'inclouen dins de la categoria de DCP, però que en atribuir-los un codi comporta que tercers no tinguin accés directe a les dades identificatives. D'aquesta manera es minimitza el risc.

El principi de minimització ha de relacionar-se amb el de conservació de les dades. De manera que es crea un principi de limitació del termini de conservació de les dades.

Lògicament, també hi ha excepcions a aquesta necessitat d'establir un límit a la conservació de les dades, com el supòsit indicat anteriorment de conservació per a una finalitat d'arxiu per a interès públic

En relació amb el termini de conservació de les dades: s'ha de tenir en compte l'exigència del RGPD i del contingut de les clàusules informatives. Ha d'informar-se del termini en què es pensa conservar les dades. Si no és possible fixar un termini, sí almenys establir els criteris que permetin determinar el termini de conservació [art. 13.2.a) i art. 14.2.a) RGPD].

Quart, les dades personals han de ser exactes i, si és necessari, actualitzades; s'han d'adoptar totes les mesures raonables perquè se suprimeixin o rectifiquin sense dilació les dades personals que siguin inexactes pel que fa a les finalitats per a les quals es tracten ("exactitud", art. 5.1.d) RGPD).

Les dades han de ser exactes i estar actualitzades. D'una altra manera han de rectificar-se o suprimir-se.

Això també està relacionat amb el deure del RT de comunicar als destinataris de les dades que s'ha produït la rectificació o supressió. Aquesta obligació es troba en el RLOPD i també està prevista en l'art. 19 RGPD.

Cinquè, les dades personals s'han de mantenir 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 poden conservar-se durant períodes més llargs sempre que es tractin exclusivament amb finalitats d'arxiu en interès públic, finalitats de recerca 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 a fi de protegir els drets i llibertats de l'interessat ("limitació del termini de conservació", art. 5.1.e) RGPD).

Sisè, les dades personals s'han detractar de 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", art. 5.1.f) RGPD).

Això representa una concreció dels articles 9 (principi de seguretat) i 10 (deure de confidencialitat) de la LOPD. Si bé el RGPD utilitza els termes d'*integritat* i *seguretat*, es tracta del principi de seguretat "revisat".

En definitiva, mitjançant mesures tècniques o organitzatives, ha de garantir-se una seguretat adequada contra el tractament no autoritzat o il·lícit, la pèrdua o la destrucció o dany accidental.

El contingut és gairebé el mateix que el de l'article 9 LOPD. Es tracta, en definitiva, de garantir una seguretat adequada respecte de la pèrdua d'informació o bé d'un dany en la informació. No obstant això, allò que és més nou no són els deures de seguretat, sinó els instruments per a fer-la efectiva:

Aquestes eines són les següents: avaluar els riscos que han d'afrontar-se en iniciar un tractament, implementar mesures tècniques i organitzatives adequades i notificar les violacions de seguretat.

> Setè, el responsable del tractament serà responsable del compliment del que disposa l'apartat 1 i capaç de demostrar-("responsabilitat proactiva", art. 5.2 RGPD).

Es tracta del nou principi incorporat; d'una responsabilitat demostrable (*accountability*). L'enfocament de la LOPD (i de la DPD) poden qualificar-se com de *reactius*. De manera que si es produeix un incompliment de la norma o un dany, el RT ha de respondre.

L'aproximació del RGPD afegeix a aquesta aproximació reactiva una de proactiva. Estableix la càrrega sobre el RT d'adoptar determinades mesures i estar en condicions de poder-ho demostrar. Es tracta, en definitiva, de retre comptes de com s'efectua el tractament. Per a això pot dotar-se de les eines que estan previstes en el capítol IV RGPD. En definitiva, de l'adopció d'una política de protecció de dades, del registre d'operacions de tractament, la protecció de dades des del disseny i protecció de dades per defecte, l'establiment i reconeixement de codis de conducta, de certificacions i segells així com l'avaluació de l'impacte sobre la protecció de dades. També s'inclouen dins d'aquestes mesures preventives la necessitat de formalitzar una consulta prèvia, els criteris i diligència en designar un ET i DPO i singularment l'adopció de mesures de seguretat. Així mateix, dins d'aquest concepte de seguretat ampli, s'inclou el deure de notificar les violacions de seguretat. Un altre aspecte que implica acreditar que s'adopta una postura diligent és que aquestes mesures han de revisar-se i actualitzar-se de manera periòdica.

En definitiva, es tracta d'un conjunt d'instruments per a fer efectiva la responsabilitat proactiva. Si bé aquesta es configura i considera com un principi, les obligacions recollides en el capítol IV són autèntiques obligacions i com a tals són exigibles al llarg de tot el tractament.

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

L'article 5.1.a) RGPD determina que el tractament ha de ser lícit, requisit que es desenvolupa en l'article 6 LOPD.

En aquest precepte es recullen els supòsits que permeten (habiliten) un tractament de dades, de manera que, si no hi ha cap d'aquestes habilitacions, el tractament no és lícit i no pot dur-se a terme. Aquest és l'esquema que ja es va establir en l'article 7.1 DPD, que determina: "els estats membres han de disposar que el tractament de dades personals *només* pugui efectuar-se si [...]".

Per tant, la possibilitat de dur a terme un tractament de dades és vista com una cosa residual, si bé són tantes les excepcions que, en la pràctica, és difícil que un supòsit no trobi cabuda dins d'alguna d'aquestes excepcions.

El RGPD segueix el mateix patró que l'art. 7 DPD, de manera que, segons disposa l'article 6.1. RGPD, "El tractament solament és lícit si es compleix almenys una de les condicions següents [...]".

> "a) l'interessat va donar el seu consentiment per al tractament de les seves dades personals per a una o diverses finalitats específiques;
>
> b) el tractament és necessari per a l'execució d'un contracte en el qual l'interessat és part o per a l'aplicació a petició d'aquest de mesures precontractuals;
>
> c) el tractament és necessari per al compliment d'una obligació legal aplicable al responsable del tractament;
>
> d) el tractament és necessari per a protegir interessos vitals de l'interessat o d'una altra persona física;
>
> e) el tractament és necessari per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament;
>
> f) el tractament és necessari 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 dades personals, en particular quan l'interessat sigui un nen.
>
> El que disposa la lletra f) del paràgraf primer no és aplicable al tractament realitzat per les autoritats públiques en l'exercici de les seves funcions.
>
> 2. Els estats membres poden mantenir o introduir disposicions més específiques a fi d'adaptar l'aplicació de les normes d'aquest Reglament pel que fa al tractament en compliment de l'apartat 1, lletres c) i e), fixant de manera més precisa requisits específics de tractament i altres mesures que garanteixin un tractament lícit i equitatiu, amb inclusió d'altres situacions específiques de tractament d'acord amb el capítol IX.
>
> 3. La base del tractament indicat en l'apartat 1, lletres c) i e), ha de ser establerta pel següent:
>
> a) el dret de la Unió, o

b) el dret dels estats membres que s'apliqui al responsable del tractament.[...]"

La primera valoració que es pot fer de l'art. 6 RGPD és que no aporta novetats substancials respecte del contingut de l'art. 7 DPD, que seria el seu equivalent. En tot cas cal destacar la possibilitat, sotmesa a cauteles, de tractar les dades per a una finalitat diferent d'aquella per a la qual es van recollir (art. 6.4 RGPD) i la regulació del consentiment del nen (art. 8 RGPD).

Quant a l'article 6 RGPD, allò més rellevant és deixar clar que sense la concurrència d'un dels supòsits previstos en el precepte no és possible dur a terme un tractament[17]. Si bé és cert que els supòsits són amplis, i quedaran pocs casos fora, ha de subratllar-se la necessitat que hi hagi una base legal.

[17]Així ho subratllen, entre molts, els autorssegüents: Heredero, Poullet, Aparicio o bé Lynskey.

Així mateix, el fet que concorri una base legal ex art. 6 RGPD no és suficient per si mateix per a poder tractar les dades, de manera que també han de complir-se necessàriament els principis de protecció de dades ex art. 5 RGPD. La vinculació entre els principis de protecció de dades i els mecanismes de legitimació (supòsits que permeten tractar les dades) es constata en la terminologia utilitzada en l'article 5.1.a (en la mesura que estableix que el tractament ha de ser lícit) i l'article 6 (la rúbrica del qual és: "Licitud del tractament"). Aquesta connexió ja la va posar en relleu Poullet i altres autors en un dels primers comentaris que es van dur a terme en el text de la DPD l'any 1997. Per tant, perquè es pugui dur a terme un tractament, això comporta que s'hagi de complir de forma cumulativa amb els article 5 i article 6 RGPD.

Lectura recomanada

Boulanger, M. H., Moreau, D., Léonard, T., Louveaux, S., Poullet, Y. i de Terwangne, C., "La protection des données à caractère personnel en droit communautaire: deuxième partie", en Journal des Tribunaux - Droit Européen, nº 41, 1997, pp. 145-155.

Així mateix, tal com va recordar el TJUE en la sentència de 24 de novembre 2011, en el cas ASNEF[18], les bases legals constitueixen una enumeració tancada, de manera que són les que són, i no constitueixen un supòsit exemplificatiu al qual puguin afegir-se altres categories.

[18]Es tracta de la STJUE, de 24 de novembre de 2011, Associació Nacional d'Establiments Financers de Crèdit (ASNEF), Federació de Comerç Electrònic i Màrqueting Directe (FECEMD) v. Administració de l'Estat, assumptes acumulats C-468/10 i C-469/10.

En conseqüència, en la implementació de la DPD, no poden afegir-se més requisits als que ja consten en el text de l'articulat. Quant a l'interès legítim cal assenyalar que la LOPD no va transposar correctament la DPD. La LOPD no va recollir en el seu articulat l'interès legítim com un mecanisme que per si sol permetés el tractament de dades, sinó que calia que a més les DCP estiguessin continguts en fonts accessibles al públic. El TJU va establir que no era possible afegir més exigències a les ja previstes i, per tant, l'interès legítim era un mecanisme suficient i la seva aplicació no podia quedar supeditada al fet que les dades constessin a més en una font accessible al públic (FAP). En definitiva, no poden afegir-se altres càrregues a les exigències existents.

3.4.1. Supòsit específic: l'interès legítim

Aquesta base legal va ser especialment analitzada pel TJUE en el cas ASNEF ja mencionat i també en el cas Google Spain. En el primer supòsit, el TJUE va analitzar si la legislació espanyola havia implementat correctament l'article 7.f) DPD, i concretament com es recollia la referència a l'interès legítim. Com

ja s'ha exposat, TJUE va contestar negativament la pregunta plantejada i va assenyalar que no es poden afegir més requisits a l'existència de l'interès legítim (com per contra havia fet el legislador espanyol, tant en la LOPD com en el RLOPD).

En el cas de Google Spain, el TJUE va estudiar quin era el fonament legal per a tractar les dades personals per part del cercador i, si bé va considerar que sí existia un interès legítim per part de l'esmentat cercador, la STJUE va dictaminar que en aquest cas havia de prevaler el dret de l'afectat.

3.4.2. Tractament de dades per a una finalitat diferent

Una novetat que introdueix l'article 6.4 RGPD és la possibilitat de tractar les dades per a una finalitat diferent de la prevista inicialment.

Si bé es disposa a l'article 5.1.b) RGPD,

> "les dades personals seran:
>
> b) recollides amb finalitats determinades, explícites i legítimes, i no es poden tractar ulteriorment de manera incompatible amb aquestes finalitats; [...]."

El principi de limitació de la finalitat que s'enuncia en aquest precepte quedaria d'alguna manera una mica diluït amb la previsió de l'article 6.4 RGPD. Aquest últim precepte permet que les dades siguin tractades per a una finalitat diferent d'aquella per a la qual es van recollir les dades personals.

> L'art. 6.4. RGPD disposa: "Quan el tractament per a un altre fi diferent d'aquell per al qual es van recollir les dades personals no estigui basat en el consentiment de la persona interessada o al Dret de la Unió o dels estats membres que constitueixi una mesura necessària i proporcional en una societat democràtica per salvaguardar els objectius indicats en l'article 23, apartat 1, el responsable del tractament, a fi de determinar si el tractament amb un altre fi és compatible amb la finalitat per al qual es van recollir inicialment les dades personals, tindrà en compte, entre altres coses: [...]".

Per a aplicar aquest precepte ha de donar-se com a pressupòsit que el nou tractament no estigui basat en el consentiment de l'interessat ni en el dret de la Unió o dels estats membres.

> S'entén que, si ja hi ha consentiment, no fa falta més justificació, perquè el consentiment és el que dóna cobertura al tractament i, si es tracta d'una norma, aquesta és la que habilita el tractament per tant, no cal cap altra causa de justificació.

En aquests casos s'atribueix al RT la facultat de valorar (podria dir-se que la responsabilitat) si el tractament amb una altra finalitat és compatible amb la finalitat per a la qual es van recollir inicialment les dades personals.

Per a això s'ha de tenir en compte,entre altres coses[19], segons disposa l'art. 6.4 RGPD:

a) qualsevol relació entre les finalitats per les quals s'hagin recollit les dades personals i les finalitats del tractament ulterior previst;

b) el context en què s'hagin recollit les dades personals, en particular pel que fa a la relació entre els interessats i el responsable del tractament;

c) la naturalesa de les dades personals, en concret quan es tractin categories especials de dades personals, de conformitat amb l'article 9, o dades personals relatives a condemnes i infraccions penals, de conformitat amb l'article 10;

d) les possibles conseqüències per als interessats del tractament ulterior previst;

e) l'existència de garanties adequades, que poden incloure el xifratge o la seudonimització.

(19)Resulta una mica sorprenent que es digui "entre altres coses", de manera que sembla que la llista d'elements a considerar no sigui tancada i es tracti per tant d'una valoració subjectiva del responsable del tractament.

Nota

Cal recordar el que s'ha dit anteriorment en relació amb els principis de protecció de dades i el fet que el RGPD sembla relativitzar una mica la "incompatibilitat" respecte de les finalitats.

El RT ha de valorar si l'ús d'una altra finalitat és compatible o no. Com valora el RT si el canvi de finalitat és possible o no? El paràmetre i el criteri els proporciona l'article 6.4 RGPD. Si bé l'aplicació d'aquest precepte molt probablement generarà dubtes tant als RT com a les pròpies APD.

Quant al canvi de finalitat, també cal tenir en compte l'article 23.2 RGPD (relatiu a les limitacions).

3.5. En particular: el consentiment

Segons disposa l'article 6.1.a) RGPD, el consentiment constitueix una de les condicions de licitud del tractament. Això és, una de les bases legals que permet el tractament de dades.

3.5.1. Característiques del consentiment

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

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

Consentiment

El consentiment ha de donar-se mitjançant un acte afirmatiu clar que reflecteixi una manifestació de voluntat lliure, específica, informada i inequívoca de l'interessat d'acceptar el tractament de dades de caràcter personal que el concerneixen, com una declaració per escrit, fins i tot per mitjans electrònics, o una declaració verbal. Això podria incloure marcar una casella d'un lloc web aInternet, escollir paràmetres tècnics per a la utilització

de serveis de la societat de la informació, o qualsevol altra declaració o conducta que indiqui clarament en aquest context que l'interessat accepta la proposta de tractament de les seves dades personals. Per tant, el silenci, les caselles ja marcades o la inacció no han de constituir consentiment. El consentiment ha de donar-se pera totes les activitats de tractament realitzades amb la mateixafinalitat. Quan el tractament tingui diverses finalitats, ha de donar-se el consentiment per a totes elles. Si el consentiment de l'interessat s'ha de donar arran d'una sol·licitud per mitjans electrònics, la sol·licitud ha de ser clara, concisa i no pertorbar innecessàriament l'ús del servei per al qual es presta.

Cal subratllar que les propostes de la Comissió i del Parlament (text d'abril 2014), en lloc de dir que el consentiment havia de ser inequívoc, deien que el consentiment havia de ser explícit. No obstant això, aquesta exigència no es va mantenir en la redacció final, que va retornar al requisit que establia la Directiva sobre la necessitat d'un consentiment inequívoc (art. 7.a DPD).

Gran part dels tractaments de dades es basen en el consentiment del subjecte afectat, i una de les maneres que tenen els subjectes de ser conscients que un responsable tracta les seves dades és que aquest últim els sol·liciti el consentiment. No obstant això, proporcionar el consentiment s'ha convertit sovint en una cosa automàtica. Això comporta que, tant si es tracta d'un consentiment explícit com d'un consentiment inequívoc, en molts casos no es garanteix la plena consciència i la voluntat de l'afectat pel tractament. Per aquest motiu ha d'adoptar-se amb cautela el recurs generalitzat a l'obtenció del consentiment.

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

La fórmula adopta l'article 4.11 RGPD rebutja el silenci com a mecanisme d'obtenció del consentiment del subjecte afectat. Això pot manifestar-se mitjançant una declaració o mitjançant "una acció afirmativa clara". En conseqüència, el mer silenci no pot considerar-se una forma d'atorgar el consentiment i per tant no habilita per a tractar els DCP.

Per exemple, l'afectat rep una comunicació en què se'l convida a subscriure's gratuïtament a una publicació i se li indica que si no contesta en un termini determinat s'entendrà que consent el tractament de determinats dades. Sobre la base de l'article 4.11 RGPD, aquesta clàusula, juntament amb la falta de resposta per part 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 el concerneixen, això no comporta en cap cas que en consenti el tractament.

Per contra, l'article 14 del Reglament que desenvolupa la LOPD (RLOPD) va atribuir precisament unes conseqüències positives al silenci si es complien determinats requisits. En conseqüència, quan resulti plenament aplicable el RGPD, aquest precepte del RLOPD no podrà utilitzar-se en la mesura que és contrari al text de la norma de la UE[20].

[20]Sobre aquest tema, vegeu Llàcer Matacás, que criticava les conseqüències positives del silenci que estableix l'article 14 RLOPD.

3.5.2. Condicions per a l'atorgament del consentiment

L'article 7 RGPD porta per rúbrica "condicions per al consentiment". En aquest precepte es regulen diferents previsions relatives al consentiment.

Acreditació del consentiment: Article 7.1 RGPD

"Quan el tractament es basa en el consentiment de l'interessat, el responsable ha de ser capaç de demostrar que aquest va consentir el tractament de les seves dades personals".

En definitiva, correspon al RT acreditar el consentiment de l'afectat.

Declaració escrita amb diferents assumptes: Article 7.2 RGPD

"Si el consentiment de l'interessat es dóna en el context d'una declaració escrita que també es refereix a altres assumptes, la sol·licitud de consentiment s'ha de presentar de manera que es distingeixi clarament dels altres assumptes, de manera intel·ligible i de fàcil accés, i utilitzant un llenguatge clar i senzill. No és vinculant cap part de la declaració que constitueixi infracció d'aquest Reglament".

El punt de partida d'aquest precepte el constitueix el supòsit en què, en el marc d'una declaració escrita o d'un negoci jurídic, s'aborden diferents aspectes de manera indistinta. L'article determina la necessitat d'identificar i separar clarament, entre les diferents disposicions, la relativa al tractament de les dades personals. Es planteja la necessitat d'atorgar el consentiment per separat, de manera que si se sol·licita el consentiment per a diferents assumptes, cada un es distingeixi clarament (art. 7.2 RGPD). La finalitat d'això és que el subjecte pugui conèixer clarament què s'està sol·licitant, i consentir una clàusula i, per exemple, rebutjar-ne una altra.

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

Revocació del consentiment: Article 7.3 RGPD

"L'interessat té dret a retirar el seu consentiment en qualsevol moment. La retirada del consentiment no afecta la licitud del tractament basada en el consentiment previ a la seva retirada. Abans de donar el consentiment, l'interessat ha de ser informat d'això. Retirar el consentiment ha de ser tan fàcil com donar-lo".

Retirar

El terme *retirar el consentiment* és el que es coneix habitualment en la teoria del negoci jurídic com a *revocació del consentiment*.

L'afectat ha de ser informat degudament d'aquesta facultat tal com s'estableix en els articles 13.2.c) i 14. 2.d) RGPD.

Totes les operacions que el RT hagi efectuat prèviament a la revocació són perfectament vàlides.

Revocació de consentiment

L'article 6.3 LOPD també estableix la facultat de revocar el consentiment quanhi hagi una causa justificada i no s'hi atribueixin efectes retroactius.

Prohibició de vinculació: Article 7.4 RGPD

"En avaluar si el consentiment s'ha donat lliurement, s'ha de tenir en compte en la major mesura possible el fet de si, entre altres coses, l'execució d'un contracte, inclosa la prestació d'un servei, se supedita al consentiment al tractament de dades personals que no són necessàries per a l'execució d'aquest contracte".

Aquesta mesura vol garantir que el consentiment sigui lliure, i recull el que es coneix en la normativa de defensa dels consumidors i usuaris com a *prohibició de vinculació*.

Per exemple, si es contracta un servei de subministrament de gas o d'electricitat, la seva prestació no pot supeditar-se al fet que l'afectat doni el consentiment per al tractament de dades relatives a les seves preferències o hàbits d'alimentació, perquè aquestes dades no són necessàries per a prestar el servei contractat.

Per tant, si el RT vol demanar dades que no sónnecessàries per a un determinat contracte, pot fer-ho sempre que: 1) en el contracte que subscrigui amb l'afectat es distingeixin convenientment les clàusules relatives al tractament de dades de la resta de les clàusules, tal com exigeix l'article 7.3 RGPD; 2) en el contracte que subscrigui es distingeixin convenientment les dades que són necessàries per a la prestació del contracte/servei i les que no ho són. 3) que no es vinculi la prestació del servei o la contractació d'un bé al tractament de dades que no siguin necessàries per al compliment del contracte subscrit, segons exigeix l'article 7.4 RGPD.

3.5.3. El consentiment dels menors

L'article 8 RGPD disposa que:

1.- Quan s'apliqui l'article 6, apartat 1, lletra *a*, en relació amb l'oferta directa a nens de serveis de la societat de la informació, el tractament de les dades personals d'un nen es considera lícit quan tingui com a mínim 16 anys. Quan el nen és menor de 16 anys, aquest tractament únicament es considera lícit si el consentiment eldóna o l'autoritza el titular de la pàtria potestat o tutela sobre el nen, i solament en la mesura en què es dóna o s'autoritza.

Els estats membres poden establir per llei una edat inferior amb aquesta finalitat, sempre que aquesta no sigui inferior a 13 anys.

2.- El responsable del tractament ha de fer esforços raonables per a verificar en aquests casos que el consentiment ha estat donat o autoritzat pel titular de la pàtria potestat o tutela sobre el nen, tenint en compte la tecnologia disponible.

3.- L'apartat 1 no afecta les disposicions generals del dret contractual dels estats membres, com les normes relatives a la validesa, formació o efectes dels contractes en relació amb un nen.

L'article 8.1 RGPD és bastant similar a l'article 13.1 RLOPD. Aquest últim estableix que:

> "Pot procedir-se al tractament de les dades dels més grans de 14 anys amb el seu consentiment, excepte quan la Llei exigeixi per a la seva prestació l'assistència dels titulars de la pàtria potestat o tutela. En el cas dels menors de 14 anys es requereix el consentiment dels pares o tutors".

Sobre la base del RGPD, el menor podria atorgar el seu consentiment si és més gran de 16 anys. Per sota d'aquesta edat seria necessari el consentiment (o l'autorització) dels pares o dels tutors. No obstant això, els estats membres poden establir una edat inferior sempre que no sigui per sota dels 13 anys.

No obstant això, malgrat les similituds, entre el text RLOPD i RGPD es constaten les diferències següents:

1) L'àmbit d'aplicació del RLOPD és més ampli que el del RGPD. El primer fa referència sense més al "tractament de les dades dels més grans de 14 anys", mentre que el RGPD preveu "l'oferta directa a nens de serveis de la SI". Per tant, el RLOPD inclou el tractament de dades fins i tot per mitjans no automàtics, per exemple en paper (pensem en les fitxes mèdiques no informatitzades), com també els tractaments automatitzats que no estiguin circumscrits a l'oferta directa de serveis de la SI.

2) Quant a l'edat, en el RLOPD,el límit s'estableix als 14 mentre que en el RGPD als 16; no obstant això, en aquest últim text pot rebaixar-se fins als 13, la qual cosa no preveu el RLOPD.

En definitiva, en el marc d'aplicació de la LOPD i del RLOPD, poden tractar-se les dades dels més grans de 14 anys amb el seu consentiment. Quan el RGPD resulti aplicable plenament, en l'ordenament jurídic espanyol, pot considerar-se que també poden seguir tractant-se les dades dels més grans de 14 anys,ja que ja existeix la norma que així ho disposa i a la qual fa la crida l'article 8.1.*infine* RGPD. L'únic dubte que pot plantejar aquesta interpretació és en el terme *llei*, en la mesura que la previsió de la rebaixa d'edat als 14 anys no està prevista en una llei sinó en un reglament.

Ha de destacar-se que el RGPD no fa referència en cap cas al supòsit dels incapacitats. Possiblement la sentència d'incapacitació establirà alguna cosa al respecte però, i si no diu res sobre aquest tema? Penseu en totes les dades de salut dels incapacitats, qui ha d'autoritzar el tractament d'aquestes dades? A falta d'una norma sobre aquest tema, i si la sentència no determina res, hauria d'atorgar-se a l'incapacitat la facultat de poder consentir, sobre la base del principi que la limitació de la capacitat ha d'interpretar-se sempre en el sentit menys restrictiu possible.

Un altre aspecte a tenir en compte és la verificació de l'edat. Segons disposa l'article 8.2 RGPD,

"El responsable del tractament ha de fer esforços raonables per a verificar en aquests casos que el consentiment ha estat donat o autoritzat pel titular de la pàtria potestat o tutela sobre el nen, tenint en compte la tecnologia disponible".

Aquest precepte és molt similar al de l'article 13.4 RLOPD. Lògicament, s'atribueix al RT un deure de posar uns mitjans raonables, no s'estableix una obligació de resultat.

3.5.4. El tractament de categories especials de dades (dades sensibles)

Com ja s'ha indicat en analitzar el terme *dada*, la gran majoria de textos legals que regulen el tractament de dades personals estableix una distinció entre tipus de dades, de manera que es considera que determinada informació ha de gaudir de més protecció. En aquesta línia, el RGPD, seguint la DPD, no tracta totes les dades de la mateixa manera, sinó que estableix una distinció.

Dins de les dades personals,el RGPD en distingeix i separa unes, les que qualifica com a "especials". No obstant això, como ja s'ha exposat, aquesta no és l'única solució per la qual hauria pogut optar el legislador. Una altra solució possible seria reconèixer i establir tipus o categories de tractaments, de manera que la dada en si mateixa no fos el que determinés un règim o un altre, sinó el tipus de tractament (sobre la base de la seva finalitat o les circumstàncies en què tingués lloc). No obstant això, el RGPD segueix el mateix patró que la DPD en establir tipologies de dades.

Dades especials

L'article 9 RGPD porta per rúbrica: "Tractament de categories especials de dades personals". Per tant, el que fa especial un tractament és el tipus de dades a les quals fa referència, i no les circumstàncies d'aquest.Aquestes dades especials també es coneixen com a *dades sensibles*.

1) Dades que tenen la categoria d'especials(art. 9 RGPD). Es tracta de les dades personals que revelin"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 dirigides a identificar de manera unívoca a una persona física, dades relatives a la salut o dades relatives a la vida sexual o l'orientació sexuals d'una persona física" (art. 9.1 RGPD).

A continuació s'exposen les diferències principals entre l'article 8 DPD i l'article 9 RGPD.

En el RGPD s'inclouen noves categories de dades respecte a les que preveu la DPD. És el cas de les dades genètiques i biomètriques. Abans de l'aprovació del RGPD,alguns autors defensaven que les dades genètiques podien considerar-se incloses dins de les dades de salut. No obstant això, ha d'admetre's que no totes

Definició de dades

Vegeu la definició de tots els tipus dades en l'article 4 RGPD.

les dades genètiques estan relacionades amb la salut. Per tant, el fet d'incloure el terme *dada genètica* comporta que ja no hi ha dubtes que queden protegides de manera especial tots aquests tipus de dades.

En altres supòsits es produeix una variació de la redacció i dels termes utilitzats.

Concretament, quant a les dades relatives a la sexualitat (DPD), el RGPD estableix el següent: dades relatives a la vida sexual o l'orientació sexual d'una persona física. Per tant, aquest últim supòsit és més ampli que el de la DPD.

Una altra categoria a tenir en compte és la relativa a les dades sobre condemnes i infraccions penals. Aquest tipus de dades, si bé no es qualifiquen com a dades sensibles, sí tenen unes peculiaritats quant al tractament. L'article 10 RGPD disposa que

> "El tractament de dades personals relatives a condemnes i infraccions penals o mesures de seguretat connexes sobre la base de l'article 6, apartat 1, només pot dur-se a terme sota la supervisió de les autoritats públiques o quan ho autoritzi el dret de la Unió o dels estats membres que estableixi garanties adequades per als drets i llibertats dels interessats. Solament pot portar-se un registre complet de condemnes penals sota el control de les autoritats públiques".

Si bé la solució que proporciona el RGPD respecte a les condemnes i infraccions penals i mesures de seguretat és molt similar a la de la DPD, no passa el mateix quant al tractament de dades relatiu a sancions administratives o processos civils. El text DPD estableix que "els estats membres poden establir que el tractament de dades relatives a sancions administratives o processos civils es dugui a terme així mateix sota el control dels poders públics". El RGPD no diu res sobre aquest tema.

2) Condicions per a tractar les dades especials (sensibles). Les condicions per a tractar les dades sensibles no difereixen gaire entre la DPD i el RGPD.

De la mateixa manera que preveu l'article 8 DPD, l'article 9 RGPD parteix d'un principi prohibitiu del tractament de les dades sensibles. L'article 9.1 RGPD determina que "queda prohibit el tractament de dades personals que revelin [...]".

No obstant això, després d'establir aquesta prohibició tan radical, s'estableix que"l'apartat 1 no és aplicable quan concorre una de les circumstàncies següents: [...]" (art. 9.2 RGPD), de manera que es pot aixecar la prohibició en els supòsits que s'enumeren a continuació.

En definitiva, de la mateixa manera que s'estableix en l'article 8 DPD, l'article 9 RGPD determina una regla general de prohibició i a continuació una relació d'excepcions a aquesta prohibició.

Article 9.2 RGPD:

"L'apartat 1 no és aplicable quan concorre una de les circumstàncies següents:

a) l'interessat ha donat el seu consentiment explícit, excepte quan el dret de la Unió o dels estats membres estableixi que la prohibició esmentada en l'apartat 1 no pot ser aixecada per l'interessat;

b) el tractament és necessari per al compliment d'obligacions i l'exercici de drets específics del responsable del tractament o de l'interessat en l'àmbit del dret laboral i de la seguretat i protecció social,

c) el tractament és necessari per a protegir interessos vitals de l'interessat o d'una altra persona física,

d) el tractament és efectuat, en l'àmbit de les seves activitats legítimes i amb les garanties degudes, per una fundació, una associació o qualsevol altre organisme sense ànim de lucre, la finalitat del qual sigui política, filosòfica, religiosa o sindical,

e) el tractament es refereix a dades personals que l'interessat ha fet públiques manifestament;

f) el tractament és necessari per a la formulació, l'exercici o la defensa de reclamacions o quan els tribunals actuïn en exercici de la seva funció judicial;

g) el tractament és necessari per raons d'un interès públic essencial, sobre la base del dret de la Unió o dels estats membres,

h) el tractament és necessari per a finalitats de medicina preventiva o laboral, avaluació de la capacitat laboral del treballador, diagnòstic mèdic, prestació d'assistència o tractament de tipus sanitari o social, o gestió dels sistemes i serveis d'assistència sanitària i social, sobre la base del dret de la Unió o dels estats membres o en virtut d'un contracte amb un professional sanitari

i) el tractament és necessari per raons d'interès públic en l'àmbit de la salut pública, com la protecció enfront d'amenaces transfrontereres greus per a la salut, o per a garantir nivells elevats de qualitat i de seguretat de l'assistència sanitària i dels medicaments o productes sanitaris, sobre la base del dret de la Unió o dels estats membres que estableixi mesures adequades i específiques per a protegir els drets i llibertats de l'interessat, en particular el secret professional,

j) el tractament és necessari amb finalitats d'arxiu en interès públic, finalitats de recerca científica o històrica o finalitats estadístiques, de conformitat amb l'article 89, apartat 1, sobre la base del dret de la Unió o dels estats membres, que ha de ser proporcional a l'objectiu perseguit, respectar en l'essencial el dret a la protecció de dades i establir mesures adequades i específiques per a protegir els interessos i drets fonamentals de l'interessat.

Quant a l'atorgament del consentiment, noteu que l'article 9.2.a) RGPD estableix l'exigència de consentiment explícit. Es considera que amb l'exigència d'un consentiment explícit, en lloc d'un consentiment inequívoc (tal com estableix l'article 4.11 RGPD com a regla general), es dóna més protecció a l'afectat en la mesura que la prestació del consentiment no és tan automàtica.

Quant a les diferències entre el contingut de l'article 8 DPD i article 9 RGPD respecte al tractament de les denominades dades sensibles, poden determinar-se les següents:

1) La manera de fer referència a les excepcions a la regla general continguda en el primer paràgraf dels articles respectius. Així, en la DPD es disposa que"no s'aplica quan", mentre que el RGPD fa referència al fet que "concorri una de les circumstàncies següents". Per tant, en el text RGPD queda clar que per a la seva aplicació n'hi ha prou que en concorri una.

2) Quant a la possibilitat d'establir excepcions, l'article 8.4 DPD determina que"Sempre que disposin les garanties adequades, els estats membres poden, per motius d'interès públic importants, establir altres excepcions, a més de les que preveu l'apartat 2, bé mitjançant la legislació nacional, bé per decisió de l'autoritat de control". Per tant, això comportaria afegir altres excepcions a les ja previstes.

Aquesta possibilitat també es preveu en l'article 9.2.g) RGPD si bé la seva redacció és una mica diferent: disposa que la prohibició de no tractar les dades sensibles no és aplicable quan"el tractament és necessari per raons d'un interès públic essencial, sobre la base del dret de la Unió o dels estats membres, que ha de ser proporcional a l'objectiu perseguit, respectar en l'essencial el dret a la protecció de dades i establir mesures adequades i específiques per a protegir els interessos i drets fonamentals de l'interessat".

No obstant això, hi ha matisos entre la redacció de l'article 8.4 DPD i la de l'article 9.2.g) RGPD, alguns dels quals són rellevants.

Excepcions en el tractament de dades

Si bé la DPD determina que són els estats els qui poden establir altres excepcions, amb la qual cosaes dedueix que com a mínim ha d'adoptar-se una disposició o regulació en què es ponderin els drets en joc i especialment l'adopció de les garanties adequades, en canvi, sobre la base del text del RGPD sembla que sense necessitat d'adoptar aquesta disposició, poden establir-se excepcions si concorre una circumstància concreta: que el tractament sigui necessari per raons d'un interès públic essencial. No obstant això, no es determina ni qui ha de dur a terme aquesta valoració, ni com ha d'adoptar-se (mitjançant quin instrument). Només es determina quins elements han de tenir-se en compte: sobre la base del dret de la Unió o dels estats membres, que ha de ser proporcional a l'objectiu perseguit, respectar en l'essencial el dret a la protecció de dades i establir mesures adequades i específiques per a protegir els interessos i drets fonamentals de l'interessat.

Per tant, l'article 9.2.g) RGPD fins i tot podria interpretar-se en el sentit que és el RT qui pot adoptar la decisió de tractar les dades sobre la base del que ell considerés un interès públic essencial. Aquesta solució no sembla la més adequada. En canvi, en el text de la DPD sembla més clar que ha d'adoptar-se una mesura legislativa abans de poder introduir una altra excepció.

A més, la redacció de la DPD estableix una garantia ulterior, en la mesura que, segons disposa l'article 8.6, "Les excepcions a les disposicions de l'apartat 1 que estableixen els apartats 4 i 5 s'han de notificar a la Comissió". Això és, una vegada establerta l'excepció, aquesta ha de notificar-se a la Comissió, amb la qual cosa sembla que hi ha un control suplementari.

3) En relació amb les dades de salut, el RGPD estableix més supòsits en què les dades poden tractar-se prescindint del consentiment explícit de l'afectat. Això en part és raonable, ja que cada vegada la casuística és més àmplia i han de preveure's més escenaris dels que la DPD va preveure inicialment. Una altra cosa és que això sigui desitjable, però d'alguna manera és una conseqüència lògica de la complexitat dels tractaments sanitaris i de la necessitat de tenir aquest tipus d'informació interconnectada.

4) Així mateix, el RGPD preveu nous supòsits recollits en els articles 9.2.f), 9.2.h), 9.2.i) i 9.2.j) RGPD.

3.6. Els subjectes que participen en el tractament de dades

Quant a l'àmbit subjectiu, resulta oportú distingir entre els subjectes que **participen del tractament** i els que el **supervisen** (les autoritats de protecció de dades i el DPO). El primer aspecte s'analitza en aquest apartat i el segon en el següent.

L'estudi dels subjectes que participen d'un tractament pot analitzar des de la perspectiva d'una relació jurídica. Aquesta relació està integrada en un dels extrems pel responsable del tractament i en l'altre per l'afectat o interessat (el subjecte a qui fan referència les dades objecte de tractament). En la majoria dels tractaments també poden participar en aquesta relació l'encarregat o subencarrregat i també pot trobar-s'hi el destinatari o destinataris i els tercers.

3.6.1. Els subjectes que tracten les dades personals

En aquesta qüestió, el RGPD no ha introduït gaires canvis i això pot ser criticable. De fet, pràcticament es produeix una continuïtat en aquest àmbit, entre la regulació de la DPD i el RGPD.

Per a alguns autors resulta qüestionable el fet que es mantingui la distinció entre responsable i encarregat del tractament, assignant al 1r. la responsabilitat principal. Tanmateix, això no sembla la solució més adequada en un context en què hi ha molts subjectes que hi intervenen i no sempre és fàcil identificar la responsabilitat de cadascun:

1) D'una banda, en determinats contextos, per exemple en la computació en el núvol, no és cert que el denominat *responsable* tingui facultat per a dirigir i decidir sempre la finalitat i l'evolució del tractament.

2) El fet de mantenir la distinció en els termes establerts sembla que sigui més un mecanisme per a proporcionar sortida als diferents actors/responsables potencials, i com un mecanisme per a eludir les seves responsabilitats. D'aquesta manera, el subjecte afectat es veu confós possiblement per no saber exactament a qui demandar.

3) Alguns autors (De Hert, per exemple) consideren que tothom qui tracta les dades hauria de tenir un mateix nivell de responsabilitat i no troben justificació en que els que participen d'alguna manera en el tractament de la informació personal no hagin de fer front a les responsabilitats respectives.

L'únic element que es valora favorablement és la introducció de la responsabilitat solidària.

En definitiva, es tracta d'un esquema (els subjectes existents i la distribució de les seves responsabilitats) ja una mica anacrònic, que no donaria resposta efectiva a la relació que s'estableix actualment i que permet eludir responsabilitats en segons quins casos, als que tracten DCP.

A continuació, s'analitzarà el règim jurídic al que estan sotmesos dels subjectes que tracten les DCP segons el RGPD.

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 d'altres, **determina les finalitats i els mitjans del tractament**; si el dret de la Unió o dels estats membres determina les finalitats i els mitjans del tractament, el responsable del tractament o els criteris específics per al seu nomenament pot establir-los el dret de la Unió o dels estats membres".

Per tant, allò que caracteritza al RT és el fet de prendre una decisió, això és, determinar les finalitats i mitjans del tractament.

El RGPD preveu i fa referència especialment als supòsits en què hi hagi més d'un RT, de manera que en aquest cas aquests subjectes són considerats com corresponsables del tractament. Així ho estableix l'article 26 RGPD, segons el qual,

> "quan dos o més responsables determinen conjuntament els objectius i els mitjans del tractament se'ls considera corresponsables del tractament. Els corresponsables han de determinar de manera transparent i de mutu acord les seves responsabilitats respectives en el compliment de les obligacions imposades per aquest Reglament, en particular quant a l'exercici dels drets de l'interessat i a les seves obligacions de subministrament d'informació a què es refereixen els articles 13 i 14, excepte, i en la mesura en què, les seves responsabilitats es regeixin pel dret de la Unió o dels estats membres que se'ls apliqui a ells. [...]" (art. 26.1 RGPD).

Aquest acord ha de reflectir degudament les funcions i relacions respectives dels corresponsables en relació amb els interessats, i els aspectes essencials d'aquest acord s'han de posar a disposició de l'interessat (art. 26.2 RGPD).

No obstant això, amb independència dels termes de l'acord, els interessats poden exercir els drets que els reconeix aquest Reglament davant de cadascun dels responsables, i en contra de cadascun d'ells (art. 26.3 RGPD).

> Per tant, l'article 26.3 RGPD sembla que dóna a entendre que en les relacions externes, davant els afectats pel tractament, s'establiria un tipus de responsabilitat solidària, de manera que qualsevol dels RT respondria del compliment de totes les obligacions. Això és, els pactes interns que poguessin establir, de distribució de les seves respectives funcions i responsabilitats, no afectarien l'esfera externa i l'exercici dels drets pels afectats.

Quant a les funcions que duu a terme el RT, aquestes es poden agrupar tenint en compte bàsicament 3 moments:

- un primer moment en què es planifica (projecta) el tractament i es determinen els mitjans del tractament,
- un segon moment en què s'efectua el tractament i
- el tercer moment de finalització del tractament.

No obstant això, abans d'analitzar les funcions del RT i les diferents etapes en les quals intervé, cal tenir en compte el canvi de perspectiva que ha representat el RGPD en relació amb la possibilitat d'iniciar un tractament de dades.

En el marc de la Directiva (DPD) calia, com a regla general, notificar a l'autoritat de control amb anterioritat a la realització d'un tractament (art. 18.1 DPD) la voluntat de dur-lo a terme. Si bé en alguns casos els estats podien disposar la simplificació o l'omissió d'aquesta notificació (art. 18.2 DPD) o que alguns tractaments fossin notificats eventualment d'una manera simplificada (art. 18.5 DPD). L'article 19 DPD fa referència al contingut d'aquesta notificació. La LOPD regula aquests deures de notificació. Quant als fitxers de titularitat pública, l'article 20 LOPD disposa que la creació, modificació o supressió dels fitxers de les AP solament poden fer-se per mitjà d'una disposició general publicada en el BOE o diari oficial corresponent.

Respecte als fitxers de titularitat privada, l'article 26.1 LOPD disposa que

> "Tota persona o entitat que procedeixi a la creació de fitxers de dades de caràcter personal **ho ha de notificar prèviament** a l'Agència de Protecció de Dades".

Es regulen determinats aspectes que ha de contenir la notificació (art. 26.2 LOPD). En qualsevol cas, el Registre general de protecció de dades ha d'inscriure el fitxer si la notificació s'ajusta als requisits exigibles o bé pot demanar que es completin les dades que faltin o que s'esmenin (art. 26.4 LOPD). Transcorregut un mes des de la presentació de la sol·licitud de la inscripció sense que l'Agència hagi emès una resolució sobre aquesta, s'entén inscrit el fitxer automatitzat amb caràcter general (arts. 26.5 LOPD).

En canvi, la perspectiva del RGPD és diferent, en principi es pot procedir al tractament de dades assumint el RT una sèrie d'obligacions. En el marc del RGPD, si es donen les condicions de legitimació previstes (art. 5 i 6 RGPD), el tractament pot dur-se a terme. En tot cas el RT, en iniciar el tractament, ha de prendre una sèrie de precaucions i ha d'assegurar-se que compleix amb la normativa. Així mateix ha de poder acreditar que això és així en cas que se sotmeti a un control per part de l'autoritat competent (principi de responsabilitat proactiva, exarticle 5.2 RGPD).

Article 5.2

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

Per tant, el RT ha de ser conscient del que vol dur a terme i valorar, abans d'iniciar un tractament, quina estratègia vol seguir (cf ha de sospesar adequadament quines dades necessita i com les tractarà, i adoptar la tecnologia que sigui més adequada).

Així mateix, quan sigui necessari, haurà de dur a terme una valoració de l'impacte que respecte de la privacitat pot comportar el tractament de dades que vol realitzar (*privacy impact assessment*). Avaluació de l'impacte relativa a la protecció de dades (art. 35 RGPD).

També ha d'implementar des d'un primer moment mesures de privacitat basades en el disseny (art. 25 RGPD) i en segons quins casos procedir a la consulta prèvia davant l'autoritat de control (art. 36 RGPD).

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

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

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

No obstant això, el conjunt de les obligacions que corresponen al RT estan definides per aquesta nova perspectiva a la qual s'ha fet referència i que representa un canvi de filosofia que pot identificar-se com "de la notificació prèvia, al principi d'*accountability*, és a dir, al principi de responsabilitat proactiva".

Els deures de notificació establerts en la DPD aviat es van descobrir una mica inútils, especialment tenint en compte la infinitat de tractaments duts a terme. A més, la idea originària que hi hauria un tractament limitat a un determinat país, sota una autoritat de control, quedava superada. Per això, al poc temps d'adoptar-se la directiva es va considerar que aquest sistema quedava una mica obsolet.

En el text del RGPD, simplement no és que s'hagi reemplaçat tècnicament la notificació per altres disposicions. Però *de facto* es pot dir que ha estat substituïda pel deure d'*accountability*.

Això és, en definitiva es produeix una inversió de la càrrega de la prova: si abans l'RT havia d'acreditar que complia davant l'autoritat, ara es tracta de desenvolupar diligentment totes les funcions encomanades a l'RT. Entre aquestes funcions destaca: tenir un registre dels tractaments efectuats; adoptar una sèrie de mesures (*privacy impact assessment* quan escaigui, més l'adopció

de mesures tecnològiques que siguin *privacy friendly* o bé fer una consulta davant l'autoritat de protecció de dades competent) i, sobre la base d'això, poder demostrar que es compleix amb la normativa de protecció de dades quan sigui requerit.

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 això comporta:

1) Abans d'iniciar el tractament:

- verificar que es compleix amb la normativa de protecció de dades;
- respectar els principis de protecció de dades;
- verificar si el tractament és lícit (té un fonament legal);
- quan sigui necessari, dur a terme una valoració de l'impacte que pot tenir, respecte de la privacitat, el tractament de dades que es vol dur a terme (*privacy impact assessment*);
- quan sigui necessari, fer la consulta prèvia a l'autoritat de protecció de dades competent;
- dotar-se dels mitjans tècnics i personals adequats;
- en cas de triar encarregats del tractament, fer-ho amb la diligència deguda i formalitzar un contracte o un altre negoci jurídic.

En qualsevol cas, ha de tenir-se en compte el canvi de perspectiva que representa l'adopció del RGPD. Un dels principis bàsics del nou marc legal és el de *data protection by design* i *data protection by default*.

El RGPD estableix noves obligacions per implementar les mesures tecnològiques que afavoreixin la privacitat des del primer moment de la concepció d'un producte/servei que comporti el tractament d'informació personal. També han de seleccionar-se les tècniques que són més protectores de la protecció de la privacitat d'un subjecte. Principis tots ells que són fonamentals per a les empreses en el moment de dissenyar nous productes.

2) Durant el tractament:

- Durant el tractament, adoptar una sèrie de garanties;
- Portar un registre de les activitats de tractament efectuades sota la seva responsabilitat, amb la informació que exigeix l'article 30.1 RGPD;
- Dotar-se dels mitjans tècnics i personals adequats;
- En cas de triar encarregats del tractament, fer-ho amb la diligència deguda i subscriure un negoci jurídic;
- Adoptar les mesures de seguretat necessàries;

- Complir amb les obligacions pròpies del responsable;
- Donar resposta a l'exercici dels drets per part de l'afectat/interessat;
- Poder demostrar que es compleix amb la normativa (principi de responsabilitat = *accountability*). Entre les maneres d'acreditar que es compleix degudament amb la normativa destaquem:
  - el fet de tenir un *privacy seal*
  - estar vinculat per unes BCR i complir-les

3) En finalitzar el tractament:

- Determinar si han de suprimir-se les dades o bé limitar-se el seu tractament;
- Fer front al possible exercici d'accions per part de l'afectat/interessat;
- Valorar si es posa fi a la relació amb l'ET i, en tot cas, veure com s'acaba (si han de retornar-se les dades o no).

Quin és el marc d'actuació del RT? Segons disposa l'article 24.1 RGPD, tenint en compte la naturalesa, l'àmbit, el context i les finalitats del tractament, així com els riscos de probabilitat i gravetat diversa per als drets i les llibertats de les persones físiques, el responsable del tractament ha d'aplicar mesures tècniques i organitzatives apropiades per garantir i poder demostrar que el tractament és conforme a aquest Reglament. Aquestes mesures s'han de revisar i actualitzar quan sigui necessari.

Per tant, el RT ha d'adoptar una sèrie de mesures en relació amb el tractament.

Per a això, quins elements ha de tenir en compte?Ha de tenir-se en compte la naturalesa, l'àmbit, el context, les finalitats del tractament, així com els riscos de probabilitat i gravetat diversa que comporta el tractament per als drets i les llibertats de les persones físiques (art. 24.1 RGPD), així com l'estat de la tècnica i el cost de l'aplicació d'aquestes mesures (art. 25.1 RGPD). Tant en el moment de determinar els mitjans de tractamen com en el moment del tractament mateix, el RT actua i pren decisions tenint en compte una sèrie d'elements: l'estat de la tècnica, el cost de l'aplicació i la naturalesa, l'àmbit, el context i les finalitats del tractament, així com els riscos de probabilitat i gravetat diversa que comporta el tractament per als drets i llibertats de les persones físiques (art. 25.1 RGPD). Per tant, aquests elements serveixen al RT com a "paràmetre" per a determinar si s'ha actuat adequadament i també lògicament s'han de tenir en compte a l'hora d'avaluar com ha exercit la seva labor.

Quines mesures han d'adoptar-se? El RT ha d'aplicar, tant en el moment de determinar els mitjans de tractament com en el moment del tractament, mesures tècniques i organitzatives apropiades (art. 24.2 i 25.1 RGPD), i entre les mesures tècniques i organitzatives apropiades s'assenyalen la seudonimització. Aquestes mesures apropiades tenen com a objectiu aplicar de manera efectiva

els principis de protecció de dades. Entre aquests principis es destaca el principi de minimització de les dades, per a poder integrar d'aquesta manera les garanties necessàries en el tractament (art. 25 RGPD).

I sobre la base d'aquests paràmetres, el RT adopta mesures tècniques i organitzatives apropiades. Concretament es consideren com a tals

> "la seudonimització, concebudes per aplicar de manera efectiva els principis de protecció de dades, com la minimització de dades, i integrar les garanties necessàries en el tractament, a fi de complir els requisits d'aquest Reglament i de protegir els drets dels interessats" (art. 25.1 RGPD).

Així mateix, es considera un element clau, a l'hora de prendre les mesures que es considerin oportunes, el respecte als principis de protecció de dades. Singularment, els principis de minimització de les dades:

> **Article 25.2**
>
> "El responsable del tractament ha d'aplicar les mesures tècniques i organitzatives apropiades amb la intenció de garantir que, per defecte, solament es tracten les dades personals que siguin necessàries per a cadascuna de les finalitats específiques del tractament. Aquesta obligació s'aplica a la quantitat de dades personals recollides, a l'abast del tractament, al termini de conservació i a la seva accessibilitat. Aquestes mesures han de garantir en particular que, per defecte, les dades personals no siguin accessibles, sense la intervenció de la persona, a un nombre indeterminat de persones físiques."

Per tant, el principi de minimització ha de complir-se en diferents moments i respecte de diferents aspectes:

- la quantitat de dades recollides
- l'extensió del tractament
- el termini de conservació/accessibilitat

I totes aquestes mesures, per a què?A fi de garantir i poder demostrar que el tractament és conforme amb aquest Reglament. Aquestes mesures es revisen i actualitzen quan és necessari (art. 24.1 RGPD) i a fi de complir els requisits d'aquest RGPD per a protegir els drets dels interessats (art. 25.1).

> **Article 25.3.**
>
> "Es pot utilitzar un mecanisme de certificació aprovat d'acord a l'article 42, com a element per acreditar el compliment de les obligacions establertes als apartats 1 i 2 d'aquest article."

D'altra banda ha de tenir-se en compte que en els casos en què el RT o l'encarregat del tractament (ET) no estan establerts en la Unió, han de designar un representant a la Unió, segons disposa l'article 27 RGPD. Aquest precepte també preveu supòsits en què no cal designar aquest representant i, en qualsevol cas, la seva designació s'ha d'entendre sense perjudici de les accions que es poden emprendre contra el mateix responsable o encarregat (art. 27.5 RGPD).

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

1) Tenir un registre. Dins del deure diligència del tractament de les DCP es troba el deure de tenir un Registre de les activitats de tractament efectuades.

L'article 30 RGPD (Registre de les activitats de tractament) disposa que:

"1. Cada responsable, o el seu representant, ha de portar un registre de les activitats de tractament efectuades sota la seva responsabilitat. Aquest registre ha de contenir tota la informació indicada a continuació:

a) el nom i les dades de contacte del responsable i, si escau, del corresponsable, del representant del responsable i del delegat de protecció de dades;

b) les finalitats del tractament;

c) una descripció de les categories d'interessats i de les categories de dades personals;

d) les categories de destinataris als qualss'han comunicat o es comunicaran les dades personals, inclosos els destinataris en tercers països o en organitzacions internacionals;

e) si escau, les transferències de dades personals a un tercer país o a una organització internacional, inclosa la identificació d'aquest tercer país o organització internacional

f) quan sigui possible, els terminis previstos per a la supressió de les diferents categories de dades;

g) quan sigui possible, una descripció general de les mesures tècniques i organitzatives de seguretat."

Article 30.3.

"Els registres a què es refereixen els apartats 1 i 2 han de constar per escrit, inclòs el format electrònic."

Article 30.4.

"El responsable o l'encarregat del tractament han de posar el registre a disposició de l'autoritat de control que ho sol·liciti."

Article 30.5.

"Les obligacions indicades en els apartats 1 i 2 no s'apliquen a cap empresa ni organització que tingui menys de 250 treballadors, tret que el tractament comporti un risc per als drets i les llibertats dels interessats, no sigui ocasional o inclogui les categories especials de dades personals indicades en l'article 9, apartat 1, o dades personals relatives a condemnes i infraccions penals a què es refereix l'article 10."

2) Cooperar amb l'Autoritat de control. El RT ha de cooperar amb l'autoritat de control quan aquesta ho sol·liciti. Així ho disposa l'art. 31 RGPD:

Article 31.

"El responsable i l'encarregat del tractament, i si escau els seus representants, han de cooperar amb l'autoritat de control que ho sol·liciti en l'acompliment de les seves funcions."

3) Deures relacionats amb la seguretat. Quant als deures de seguretat, el RGPD introdueix una nova perspectiva: la del risc. En base a aquesta correspon al RT identificar els riscos a què pot estar sotmès el tractament de la informació personal per poder-los prevenir.

L'aproximació basada en el risc consisteix a ajustar les obligacions relatives al tractament de dades als riscos que presenta un determinat tractament de dades a fi d'establir mecanismes adequats de processament de la informació. Per a aquesta valoració es té en compte la naturalesa, el context i la finalitat del tractament, així com la probabilitat i la gravetat dels riscos que un tractament pot representar per als drets i les llibertats dels individus.

Es té en compte un doble nivell d'aproximació des del risc. Algunes obligacions solament resulten aplicables a les activitats que comporten un risc elevat per a les DCP. En aquest sentit, s'estableixen obligacions com dur a terme un *data protection impact assessment*, notificar als afectats les violacions de dades o bé la consulta prèvia a les ADP.

La perspectiva del risc apareix de nou a les disposicions relatives a *privacy by design i by default*, la designació d'un representant, requisits relatius a la documentació del tractament, així com respecte de l'adopció de les mesures de seguretat.

En aquest sentit, cal proporcionar una sèrie de guies i pautes a les empreses per a ajudar-les a ser conscients del nivell de risc que el tractament de dades personals pot comportar.

Article 32. Seguretat del tractament

"1. Tenint en compte: l'estat de la tècnica, els costos d'aplicació i la naturalesa, l'abast, el context i les finalitats del tractament, així com riscos de probabilitat i gravetat variables per als drets i les llibertats de les persones físiques, el responsable i l'encarregat del tractament han d'aplicar mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat al risc, que si escau inclogui, entre d'altres:

a) la seudonimitzaciói el xifratge de dades personals;

b) la capacitat de garantir la confidencialitat, la integritat, la disponibilitat i la resiliència permanents dels sistemes i dels serveis de tractament;

c) la capacitat de restaurar la disponibilitat i l'accés a les dades personals de manera ràpida, en cas d'incident físic o tècnic;

d) un procés de verificació, avaluació i valoració regulars de l'eficàcia de les mesures tècniques i organitzatives per garantir la seguretat del tractament.

2. En avaluar l'adequació del nivell de seguretat, cal tenir particularment en compte els riscos que presenta el tractament de dades, en particular com a conseqüència de la destrucció, la pèrdua o l'alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o l'accés no autoritzats a aquestes dades.

3. L'adhesió a un codi de conducta aprovat d'acord amb l'article 40, o a un mecanisme de certificació aprovat segons l'article 42, pot servir d'element per demostrar el compliment dels requisits que estableix l'apartat 1 d'aquest article.

4. El responsable i l'encarregat del tractament han de prendre mesures per garantir que qualsevol persona que actua sota l'autoritat del responsable o de l'encarregat i que té

accés a dades personals solament pot tractar aquestes dades seguint instruccions del responsable, tret que hi estigui obligada en virtut del dret de la Unió o dels estats membres."

Mesures de seguretat en el RLOPD

Quant a les mesures de seguretat que preveu el RLOPD, vegeu el títol VIII d'aquest reglament, la rúbrica del qual és "De les mesures de seguretat en el tractament de dades de caràcter personal".

Quant a l'aplicació de les mesures de seguretat, en el context espanyol, ha de tenir-se en compte el RLOPD, que regula aquests aspectes. D'entrada, i fins que no resulti aplicable el RGPD, lògicament són aplicables les mesures que preveu el RLOPD. Així mateix, en la mesura en què no entrin en contradicció amb el RGPD també són aplicables a partir del 25 de maig de 2018.

Una novetat important que ha introduït el RGPD és el deure de notificar les fallades de seguretat, regulat en els articles 33 i 34 RGPD.

- Aquests preceptes distingeixen, d'una banda, entre el deure de notificar una violació de la seguretat de les dades personals a l'autoritat de control (art. 33) i

- la comunicació d'una violació de la seguretat de les dades personals a l'interessat (art. 34).

Quant a la notificació de la violació de la seguretat de les dades a l'autoritat de control:

- La regla general és que, en cas d'una violació de la seguretat, el responsable del tractament l'ha de notificar a l'autoritat de control competent sense dilació indeguda i, si és possible, com a tard 72 hores després que n'hagi tingut constància, tret que sigui improbable que aquesta violació de la seguretat constitueixi un risc per als drets i les llibertats de les persones físiques. Si la notificació a l'autoritat de control no té lloc en el termini de 72 hores, ha d'anar acompanyada dels motius de la dilació (art. 33.1 RGPD).

- Així mateix, l'encarregat del tractament ha de notificar sense dilació indeguda al responsable del tractament les violacions de la seguretat de les quals tingui coneixement (art. 33.2 RGPD).

Article 33.4 RGPD

"3. La notificació que preveu l'apartat 1, com a mínim, ha de fer el següent:

a) descriure la naturalesa de la violació de la seguretat de les dades personals, i també, quan sigui possible, les categories i el nombre aproximat d'interessats afectats, i les categories i el nombre aproximat de registres de dades personals afectats;

b) comunicar el nom i les dades de contacte del delegat de protecció de dades o d'un altre punt de contacte en el qual pugui obtenir-se més informació;

c) descriure les possibles conseqüències de la violació de la seguretat de les dades personals;

d) descriure les mesures adoptades o propostes pel responsable del tractament per posar remei a la violació de la seguretat, incloent, si escau, les mesures adoptades per mitigar els possibles efectes negatius.

Si no fos possible facilitar la informació simultàniament, i en la mesura en què no ho sigui, la informació s'ha de proporcionar de manera gradual."

El responsable del tractament ha de documentar qualsevol violació de la seguretat de les dades personals, inclosos els fets relacionats amb aquesta, els seus efectes i les mesures correctives que s'hagin adoptat. Aquesta documentació permet a l'autoritat de control verificar el compliment del que disposa aquest article (art. 33.5 RGPD).

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

La comunicació a l'interessat no ha de fer-se en tots els casos, sinó "quan sigui probable que la violació de la seguretat de les dades personals comporti un risc alt per als drets i les llibertats de les persones físiques", en aquest cas el RT l'ha de comunicar a l'interessat sense dilació indeguda (art. 34.1 RGPD).

La comunicació a l'interessat ha de descriure en un llenguatge clar i senzill la naturalesa de la violació de la seguretat, i ha de contenir com a mínim la informació i les mesures a què es refereix l'article 33.3, lletres b), c) i d) (art. 34.2 RGPD).

Com s'ha indicat, no sempre ha de complir-se el deure de comunicació a l'interessat. Concretament, aquesta no és necessària si es compleix alguna de les condicions següents (art. 34.3 RGPD):

a) el responsable del tractament ha adoptat les mesures de protecció tècniques i organitzatives apropiades i les ha aplicat a les dades personals afectades per la violació de la seguretat de les dades personals, en particular les que facin inintel·ligibles les dades personals per a qualsevol persona que no estigui autoritzada a accedir-hi, com el xifrat;

b) el responsable del tractament ha pres mesures ulteriors que garanteixen que ja no existeix la probabilitat que es concreti l'alt risc per als drets i les llibertats de l'interessat a què es refereix l'apartat 1.

c) suposa un esforç desproporcionat. En aquest cas, cal optar en el seu lloc per una comunicació pública o una mesura semblant, que informi els interessats de manera igualment efectiva.

Quan el responsable encara no ha comunicat a l'interessat la violació de la seguretat, l'autoritat de control, una vegada considerada la probabilitat que aquesta violació comporti un alt risc, pot exigir-li que ho faci o bé que adopti determinades mesures (art. 34.4 RGPD).

4) L'avaluació d'impacte relativa a la protecció de dades.

Una altra novetat que incorpora el RGPD és la necessitat de dur a terme, en determinats supòsits, una avaluació de l'impacte relativa a la protecció de dades. Aquesta mesura s'incardina en la filosofia a la qual ja s'ha fet referència, relacionada amb el principi de responsabilitat proactiva (art. 5.2 RGPD).

Ja s'ha assenyalat el canvi de perspectiva que ha suposat el RGPD, de manera que s'ha evolucionat d'un deure d'haver de demanar autorització per dur a terme un tractament, a la responsabilitat del RT que comporta, entre altres aspectes, valorar si es pot efectuar el tractament previst i en tot cas complir amb les exigències legals.

Segons disposa l'article 35 RGPD,

"1. Quan sigui probable que un tipus de tractament, en particular si utilitza noves tecnologies, i tenint en compte la seva naturalesa, abast, context o finalitats, pot comportar un alt risc per als drets i les llibertats de les persones físiques, abans del tractament el responsable ha d'avaluar l'impacte de les operacions de tractament en la protecció de dades personals. Una única avaluació pot abordar una sèrie d'operacions de tractament similars que comportin alts riscos similars.

2. El responsable del tractament ha de demanar l'assessorament del delegat de protecció de dades, si ha estat nomenat, en realitzar l'avaluació d'impacte relativa a la protecció de dades.

3. L'avaluació d'impacte relativa a la protecció de les dades s'ha de requerir en particular en els casos següents:

a) avaluació sistemàtica i exhaustiva d'aspectes personals de persones físiques basada en un tractament automatitzat, com l'elaboració de perfils, sobre la base de la qual es prenen decisions que produeixen efectes jurídics per a les persones físiques o que les afecten significativament de manera similar;

b) tractament a gran escala de les categories especials de dades a què es refereix l'article 9, apartat 1, o de les dades personals relatives a condemnes i infraccions penals a què es refereix l'article 10, o

c) observació sistemàtica a gran escala d'una zona d'accés públic.

4. L'autoritat de control ha d'establir i publicar una llista dels tipus d'operacions de tractament que requereixen una avaluació d'impacte relativa a la protecció de dades.

5. L'autoritat de control també pot establir i publicar la llista dels tipus de tractament que no requereixen avaluacions d'impacte.

6. Abans d'adoptar les llistes, l'autoritat de control competent ha d'aplicar el mecanisme de coherència si aquestes llistes inclouen activitats de tractament que tinguin relació amb l'oferta de béns o serveis als interessats o amb l'observació del seu comportament en diversos estats membres, o activitats de tractament que puguin afectar substancialment la lliure circulació de dades personals a la Unió.

7. L'avaluació ha d'incloure com a mínim:

a) una descripció sistemàtica de les operacions de tractament previstes i de les finalitats del tractament, inclòs, siescau, l'interès legítim perseguit pel responsable del tractament;

b) una avaluació de la necessitat i la proporcionalitat de les operacions de tractament pel que fa a la seva finalitat;

c) una avaluació dels riscos per als drets i les llibertats dels interessats;

d) les mesures previstes per afrontar els riscos.

8. El compliment dels codis de conducta pels responsables o encarregats corresponents es tindrà degudament en compte en avaluar les repercussions de les operacions de tractament efectuades per aquests responsables o encarregats.

9. Si escau, el responsable ha de recollir l'opinió dels interessats o dels seus representants en relació amb el tractament previst.

[...]

11. En cas necessari, el responsable ha d'examinar si el tractament es fa d'acord amb l'avaluació d'impacte relativa a la protecció de dades, almenys quan hi hagi un canvi del risc que representen les operacions de tractament."

PIA

La noció d'avaluació d'impacte relativa a la protecció de dades (art. 35 RGPD) és més coneguda per les seves sigles en anglès PIA i prové del dret mediambiental i de la responsabilitat pels danys al medi ambient. L'avaluació d'impacte ha de dur-se a terme, segons el parer del responsable mateix del tractament, i segons la seva valoració personal, quan aquest responsable consideri que el tractament pot comportar un risc rellevant respecte dels drets i les llibertats del subjecte. Els casos en què això pot succeir estan enumerats en el RGPD, així mateix, hi ha uns casos en què aquest risc ja existeix de per si. Es tracta de supòsits de *profiling*, o bé de seguiment sistemàtic de la persona. També en el tractament de dades sensibles.

En qualsevol cas, el PIA ha de fer-se abans de dur a terme el tractament.

L'evolució del text, des de la seva presentació per part de la Comissió, ha sofert pocs canvis. Potser el més remarcable és la possibilitat de dur a terme PIA per sectors, de manera que les PIMES no pateixin gaires perjudicis pel cost que aquests PIA comporten. Concretament es disposa que un sol PIA (una sola valoració) pot ser suficient per a tractaments semblants que presenten un risc similar. Per això es disposa que alguns PIA poden tenir un abast horitzontal, a fi de cobrir operacions similars de tractament, assumint d'alguna manera el paper d'un codi de conducta per a un sector determinat.

Això pot considerar-se un intent molt positiu d'alleugerir la càrrega que té per a les PIMES el cost financer de la implementació del RGPD i proporcionar flexibilitat.

5) Consulta prèvia. Una altra de les mesures relacionades amb aquest nou enfocament del rol del RT és la necessitat de dur a terme una consulta prèvia (art. 36 RGPD). Tanmateix, això no representa una novetat tan radical si es té en compte que l'article 20 DPD ja preveia una mesura similar en determinats casos.

L'article 20 DPD disposa que

"1. Els estats membres han de precisar els tractaments que puguin comportar riscos específics per als drets i les llibertats dels interessats i han de vetllar perquè siguin examinats abans del començament del tractament.

2. Aquestes comprovacions prèvies les ha de fer l'autoritat de control una vegada que ha rebut la notificació del responsable del tractament o bé l'encarregat de la protecció de dades, que, en cas de dubte, ha de consultar a l'autoritat de control.

3. Els estats membres també poden dur a terme aquesta comprovació en el marc de l'elaboració d'una norma aprovada pel Parlament o basada en la mateixa norma, que defineixi el caràcter del tractament i estableixi les garanties oportunes."

L'article 36 RGPD preveu que:

"1. El responsable consultarà a l'autoritat de control abans de procedir al tractament quan una avaluació d'impacte relativa a la protecció de les dades, en virtut de l'article 35, mostra que el tractament comporta un alt risc si el responsable no pren mesures per mitigar-lo.

2. Quan l'autoritat de control considera que el tractament previst aquè es refereix l'apartat 1 pot infringir aquest Reglament, en particular quan el responsable no ha identificat o mitigat suficientment el risc, l'autoritat de control, en un termini de vuit setmanes des de la sol·licitud de la consulta, ha d'assessorar per escrit el responsable, i si escau l'encarregat, i pot utilitzar qualsevol dels seus poders esmentats en l'article 58. Aquest termini pot prorrogar-se.

3. Quan consulti a l'autoritat de control de conformitat amb l'apartat 1, el responsable del tractament li ha de facilitar la informació següent:

a) si escau, les responsabilitats respectives del responsable, dels corresponsables i dels encarregats implicats en el tractament, en particular en cas de tractament dins d'un grup empresarial;

b) les finalitats i els mitjans del tractament previst;

c) les mesures i garanties establertes per protegir els drets i les llibertats dels interessats de conformitat amb aquest Reglament;

d) si escau, les dades de contacte del delegat de protecció de dades;

e) l'avaluació d'impacte relativa a la protecció de dades que estableix l'article 35;

f) qualsevol altra informació que sol·liciti l'autoritat de control.

[...]

5. No obstant el que disposa l'apartat 1, el dret dels estats membres pot obligar els responsables del tractament a consultar l'autoritat de control i a obtenir-ne l'autorització prèvia en relació amb el tractament efectuat per un responsable en l'exercici d'una missió realitzada en interès públic, en particular el tractament en relació amb la protecció social i la salut pública."

Quant a les diferències entre l'article 20 DPD i l'article 36 RGPD, potser la diferència més notable entre un supòsit i l'altre és que, en el cas de la DPD, aquest deure de control pesa sobre l'autoritat de protecció: "comprovacions prèvies han de ser fetes per l'autoritat de control una vegada que hagi rebut la notificació del RT [...]." En canvi, en el marc del RGPD sembla que és el RT qui ha de sotmetre'l a aquesta consulta. És a dir, que la iniciativa correspon al RT en aquest darrer supòsit.

L'article 20 DPD fa referència a: "controls previs" i l'article 36 RGPD a consulta prèvia; no obstant això, hi ha algun element similar. El fet que davant determinats tractaments, que són susceptibles de generar una major amenaça per als drets i les llibertats dels subjectes, s'hagi de consultar l'autoritat de protecció de dades corresponent.

6) Designació de l'encarregat del tractament (ET).

Quant a la possibilitat de designar un ET, s'ha de tenir en compte l'article 28 RGPD.

> **Article 28.1.**
>
> "Quan s'ha de fer un tractament per compte d'un responsable del tractament, s'ha d'escollir únicament un encarregat que ofereixi garanties suficients per aplicar mesures tècniques i organitzatives apropiades, de manera que el tractament sigui conforme als requisits d'aquest Reglament i garanteixi la protecció dels drets de l'interessat".

Aquest aspecte s'analitza en el subapartat següent. En definitiva, l'art. 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 tracta 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.

Segons disposa l'article 28.1 RGPD, quan s'ha de fer un tractament per compte d'un responsable del tractament, s'ha d'escollir únicament un encarregat que ofereixi garanties suficients per aplicar mesures tècniques i organitzatives apropiades, de manera que el tractament sigui conforme als requisits d'aquest Reglament i garanteixi la protecció dels drets de l'interessat.

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

Així mateix, segons l'article 28.3 RGPD, aquest contracte o acte jurídic ha d'estipular, en particular, que l'encarregat:

a) tracta les dades personals únicament seguint instruccions documentades del responsable;

b) garanteix que les persones autoritzades per tractar dades personals s'han compromès a respectar-ne la confidencialitat o estan subjectes a una obligació de confidencialitat de naturalesa estatutària;

c) pren totes les mesures necessàries de conformitat amb l'article 32 (relatives a la seguretat del tractament);

d) en cas de recórrer a un subencarregat del tractament, ha de respectar les exigències previstes en els articles 28.2 i 28.4;

e) assisteix el responsable, tenint en compte la naturalesa del tractament, mitjançant les mesures tècniques i organitzatives apropiades;

f) ajuda el responsable a garantir el compliment de les obligacions que estableixen els articles 32 a 36 (seguretat del tractament, comunicació de violació de seguretat i avaluació d'impacte);

g) suprimeix o retorna totes les dades personals una vegada finalitza la prestació dels serveis de tractament, i suprimeix les còpies existents tret que es requereixi la conservació de les dades personals;

h) ha de posar a disposició del responsable tota la informació necessària per demostrar que compleix les obligacions establertes en aquest article, així com permetre i contribuir a la realització d'auditories.

En qualsevol cas, l'ET no és un mer executor de les ordres del RT, ja que com disposa l'article 28.3. *infine*,

> "l'encarregat ha d'informar immediatament el responsable si, en la seva opinió, una instrucció infringeix aquest Reglament o altres disposicions en matèria de protecció de dades de la Unió o dels estats membres".

Així mateix, quant al contracte subscrit entre RT i ET, ha de tenir-se en compte que sense perjudici que el responsable i l'encarregat del tractament subscriguin un contracte individual, el contracte o un altre acte jurídic pot basar-se, totalment o parcialment, en les clàusules contractuals tipus (art. 28.6. RGPD). Així mateix aquest contracte o acte jurídic ha de constar per escrit, inclòs en format electrònic (art. 28.9).

De la mateixa manera que el RT té l'obligació de portar un registre del tractament, l'ET també ha de fer-ho, tal com disposa l'article 30.2 RGPD, cada encarregat ha de portar un registre de totes les categories d'activitats de tractament efectuades per compte d'un responsable que contingui:

a) el nom i les dades de contacte de l'encarregat i del RT per compte del qual actuï, i del delegat de protecció de dades;

b) les categories de tractaments efectuats per compte de cada responsable;

c) si escau, les transferències de dades personals a un tercer país o a una organització internacional;

d) quan sigui possible, una descripció general de les mesures tècniques i organitzatives de seguretat.

Tal com s'estableix respecte del RT, aquest registre ha de constar per escrit (fins i tot en format electrònic), ex art. 30.3 RGPD, i l'ET ha de posar el registre a disposició de l'autoritat de control que ho sol·liciti (art. 30.4 RGPD).

En tot cas, ha de tenir-se en compte que l'obligació de portar el registre no és exigible a determinades empreses o organitzacions.

Concretament, no és exigible a les que tinguin menys de 250 treballadors, tret que el tractament que realitzi pugui comportar un risc per als drets i les llibertats dels interessats, no sigui ocasional o inclogui les categories especials de dades personals esmentades en l'art. 9.1 RGPD, o les dades personals relatives a condemnes i infraccions penals a què es refereix l'article 10 RGPD (art. 30.5 RGPD).

La possibilitat que l'ET recorri a un altre ET (en definitiva en subcontracti les funcions) està especialment prevista en el RGPD. Segons disposa l'article 28.2, l'ET pot recórrer a un altre encarregat si té l'autorització prèvia per escrit, específica o general, del responsable. L'ET ha d'informar el responsable de qualsevol canvi previst en la incorporació o la substitució d'altres encarregats i, d'aquesta manera, donar al RT l'oportunitat d'oposar-se a aquests canvis.

Segons l'article 28.4 RGPD, quan un encarregat del tractament recorre a un altre encarregat per dur a terme determinades activitats de tractament per compte del responsable, cal imposar a aquest altre encarregat, mitjançant un contracte o un altre acte jurídic, les mateixes obligacions de protecció de dades que les estipulades en el contracte o un altre acte jurídic entre el responsable i l'encarregat (això és, el primer contracte que s'ha formalitzat), en particular la prestació de garanties suficients d'aplicació de mesures tècniques i organitzatives apropiades, de manera que el tractament sigui conforme amb les disposicions del RGPD. Si aquest altre encarregat (es tracta d'un subencarregat) incompleix les obligacions de protecció de dades, l'encarregat inicial continua sent plenament responsable davant el responsable del tractament pel que fa al compliment de les obligacions de l'altre encarregat.

Quant a la responsabilitat de l'ET, ha de tenir-se en compte que l'adhesió de l'encarregat del tractament a un codi de conducta aprovat d'acord amb l'exarticle 40 RGPD o d'acord amb un mecanisme de certificació aprovat segons l'exarticle 42, pot utilitzar-se com a element per demostrar que hi ha les garanties suficients (art. 28.5).

Així mateix, si un ET infringeix aquest Reglament en determinar les finalitats i mitjans del tractament, se l'ha de considerar responsable pel que fa a aquest tractament (art. 28.10).

Sobre l'obligació de diligència en el tractament de dades, cal tenir en compte que, finalment, qualsevol subjecte que tracti dades ha de fer-ho amb una determinada diligència. Això es desprèn, en primer lloc, del principi d'integritat i de confidencialitat recollit en l'article 5.1.f) RGPD:

> "Les dades personals han de ser tractades de manera que se'n garanteixi una seguretat adequada, inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la seva pèrdua, destrucció o dany accidental, mitjançant l'aplicació de les mesures tècniques o organitzatives apropiades."

Aquest principi d'integritat i confidencialitat es concreta en l'article 29 RGPD que disposa que

> "l'encarregat del tractament i qualsevol persona que actua sota l'autoritat del responsable o de l'encarregat i té accés a dades personals solament pot tractar aquestes dades seguint instruccions del responsable, tret que hi estigui obligat en virtut del dret de la Unió o dels estats membres".

En definitiva, quant a la relació entre RT i ET, ha de tenir-se en compte el següent:

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

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

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

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

5) El contracte o l'acte jurídic ha de constar per escrit, inclòs en format electrònic.

6) La fi de la prestació implica esborra o tornar les dades, sense incloure la transferència a un altre encarregat.

7) Obligació d'informar el responsable "si, en la seva opinió, una instrucció infringeix aquest Reglament o les disposicions nacionals o de la Unió en matèria de protecció de dades".

8) Possibilitat d'utilitzar contractes model.

Altres subjectes

El RGPD preveu 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 qualsevol altre organisme al qual es comuniquen dades personals, tant si és un tercer com no. No obstant això, no es consideren destinataris les autoritats públiques que poden rebre dades personals en el marc d'una investigació concreta de conformitat amb el dret de la Unió o dels estats membres; el tractament d'aquestes dades per aquestes autoritats públiques és conforme a les normes en matèria de protecció de dades aplicables a les finalitats del tractament.

Això està relacionat amb els deures d'informació. En informar el subjecte afectat pel tractament ha d'indicar-se els possibles destinataris de les dades. A aquest efecte, les autoritats públiques no es consideren destinataris i, per tant, no ha d'informar-se de la transmissió de dades en els supòsits que preveu l'article 4.9 RGPD.

D'altra banda, quant a la figura del **tercer**, l'article 4.10) RGPD reconeix com a tal: la persona física o jurídica, autoritat pública, servei o organisme diferent de l'interessat, del responsable del tractament, de l'encarregat del tractament i de les persones autoritzades per tractar les dades personals sota l'autoritat directa del responsable o de l'encarregat.

3.6.2. Els subjectes afectats pel tractament

Es tracta dels subjectes afectats o interessats respecte als que es tracten les dades.

Entre les definicions que recull l'article 4 RGPD no n'hi ha cap que faci referència a l'interessat o afectat (tampoc no n'hi havia en l'article 2 DPD de 1995, en l'elenc de definicions que es proporcionen). En qualsevol cas es tracta de la persona a qui fa referència el tractament. En quant 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 resulta aplicable a les persones jurídiques.

Els interessats o afectats tenen una sèrie de drets que s'analitzaran més endavant. També cal preguntar-nos fins a quin punt tenen deures. Per exemple, tenen el deure de proporcionar dades que no siguin falses? Així mateix, en determinats entorns, tenen el deure de tractar les dades a les quals tinguin accés, cf xarxes socials, de manera diligent? Sembla que aquesta última qüestió no quedaria resolta pel RGPD en la mesura que aquesta norma exclou del seu àmbit d'aplicació els tractaments amb finalitats domèstiques. Per tant, els subjectes que participen en una xarxa social a nivell domèstic (relacions familiars o d'amistat) quedarien fora del conjunt d'obligats a complir amb els deures que exigeix el RGPD. En tot cas, els conflictes que es puguin suscitar han de resoldre's d'acord amb les normes generals (per exemple, acudint a les regles relatives a la responsabilitat civil contingudes en el Codi civil o bé a la L'1/82 en cas de lesionar els drets a l'honor, la intimitat o la imatge d'un altre subjecte).

Alguns autors han defensat que els deures d'*accountability* també serien exigibles als subjectes afectats pel tractament, això és, que els seria exigible un determinat nivell de diligència. No obstant això, és una qüestió que el RGPD no aborda.

3.7. La supervisió del tractament

En aquest subapartat s'analitzen dos aspectes: les autoritats de protecció i el delegat deprotecció de dades (DPO, segons les sigles en anglès).

3.7.1. Les autoritats de protecció de dades

L'article 8 de la CDFUE, després de reconèixer que "tota persona té dret a la protecció de les dades de caràcter personal que la concerneixen" (art. 8.1), disposa que "el respecte d'aquestes normes queda subjecte al control d'una autoritat independent".

Les autoritats de protecció (APD) ja regulades en la DPD (art. 28) constitueixen un pilar bàsic en la implementació del Reglament, i per això en aquest text s'inclouen un conjunt d'articles destinats a aprofundir en la seva labor de coordinació per aconseguir la coherència en l'aplicació del reglament en la UE.

El RGPD comporta un reforçament del rol de les autoritats de control. La regulació d'aquestes es troba 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 RGPD, l'"autoritat de control" és l'autoritat pública independent establerta per un estat membre de conformitat 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 al grup de l'article 29, creat precisament per l'article 29 DPD i que ha desenvolupat una labor encomiable d'interpretació i d'aclariment de l'articulat de la Directiva.

Un altre aspecte al qual ha hagut de donar resposta el RGPD és al creixent 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 d'altres Estats.

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

El RGPD estableix un sistema complex per a determinar quina autoritat és la competent per a decidir sobre un assumpte, en virtut de si hi ha punts de connexió en un sol estat o en múltiples estats, en funció d'on es trobi l'afectat i el RT (secció 2 del capítol VI). Sobre la base d'aquests criteris, en els assumptes que afecten més d'un estat es determina qui és l'autoritat de control principal, que pot demanar l'ajuda d'altres autoritats afectades. Per això s'estableix un mecanisme de cooperació entre autoritats (art. 60 a 62).

L'article 4.22 RGPD defineix l'"autoritat de control interessada" com l'autoritat de control a la qual afecta el tractament de dades personals a causa del següent: a) el responsable o l'encarregat del tractament està establert al territori de l'estat membre d'aquesta autoritat de control; b) els interessats que resideixen a l'estat membre d'aquesta autoritat de control es veuen substancialment afectats o és probable que es vegin substancialment afectats pel tractament, o c) s'ha presentat una reclamació davant aquesta autoritat de control.

En la mesura que les autoritats de protecció han de prendre decisions que poden afectar l'aplicació uniforme del Reglament (per exemple, aprovació de codis de conducta, determinació de tractaments que requereixen fer una valoració de l'impacte, autorització de transferències de dades), cal assegurar-se que les decisions preses comparteixen uns mateixos criteris. Per a assegurar-ho s'estableix un procediment de coherència (art. 63 a 67), de manera que davant

determinades qüestions i matèries plantejades, les autoritats de control han de demanar un dictamen del Comitè Europeu de Protecció de Dades, i aquest ha de comunicar determinades decisions a la Comissió.

En relació amb els mecanismes de consistència, és competència del Comitè Europeu de Protecció de Dades establir els criteris per a aconseguir aquests mecanismes de consistència i de coherència i cooperació. De manera que, en molts casos, les autoritats han de sol·licitar l'opinió prèvia d'aquest Comitè i justificar si s'aparten de la seva opinió.

El Comitè de Protecció de Dades

L'article 29 DPD va crear un grup de protecció de les persones respecte al tractament de dades personals denominat Grup de l'Article 29, que té caràcter consultiu i independent. La labor i el rol que ha dut a terme aquest grup ha estat fins ara d'una grandíssima rellevància. Els seus integrants eren membres de les diferents APD nacionals, de manera que les seves decisions eren seguides ràpidament pels diferents estats. Una prova de la seva influència es troba en el seu paper relatiu a múltiples qüestions, des del mateix concepte de *dada de caràcter personal*, les responsabilitats atribuïdes al RT i ET, les posicions adoptades respecte a l'Internet de les coses, les dades massives (*big data*), la informàtica en núvol (*cloud computing*), la delimitació de l'interès legítim com a causa d'habilitació del tractament, l'adopció de criteris respecte a l'exercici del dret a l'oblit o la negociació de transferències internacionals de dades després de l'anul·lació del *safe harbour* (com a conseqüència del cas *Schrems*).

No obstant això, després de l'aprovació del RGPD, havia de dotar-se aquest grup consultiu i independent d'un nou marc, especialment perquè el RGPD haurà d'implementar-se a vint-i-nou estats i per a això cal garantir la coherència entre els diferents ordenaments.

L'article 68 RGPD crea el Comitè Europeu de Protecció de Dades (European Data Protection Board), identificat com a Comitè, com a organisme de la Unió, que gaudirà de personalitat jurídica. Aquest Comitè està representat pel seu president i compost pel director d'una autoritat de control de cada estat membre i pel supervisor europeu de protecció de dades o els seus representants respectius.

El mecanisme de coherència adoptat funciona de manera que les APD, abans d'adoptar cap decisió important, han de dirigir-se al Comitè, a qui també s'atorguen mecanismes per a dirimir controvèrsies entre les diferents autoritats implicades.

Així mateix, el Comitè conserva i amplia les facultats consultives que tenia el grup de l'article 29. Especialment importants són les competències relatives a la certificació.

En general, pot dir-se que el Comitè s'ha convertit en l'autoritat i el cos més important en matèria de protecció de dades en el territori comunitari. Aquest reforç ha anat incrementant-se respecte del text presentat inicialment per la Comissió. Aquesta, en la proposta de gener de 2012 tenia reservat bastant poder i control i tenia en bastants casos l'última paraula mitjançant la possibilitat de dictar actes delegats. Gradualment, en el procés d'adopció del Reglament, el paper del Comitè ha anat guanyant pes i incrementant-se. Potser pot afirmar-se que ha aconseguit el poder que la Comissió s'havia reservat per a ella mateixa inicialment.

3.7.2. El delegat de protecció de dades

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

El RGPD no regula quin tipus de titulació ha de tenir el subjecte que exerceixi les funcions de DPO. En qualsevol cas, ha de tractar-se de persones qualificades, que tinguin un potencial lideratge en el si de les organitzacions. L'objectiu és controlar la informació personal per a protegir-la en totes les fases del tractament.

Ha de controlar-se adequadament la informació personal per a garantir els drets de les persones que el RGPD atorga.

Així mateix, la normativa obliga a la divulgació d'aquest dret.

Article 37. Designació del delegat de protecció de dades

"1. El responsable i l'encarregat del tractament han de designar un delegat de protecció de dades sempre quan:

a) el tractament el dugui a terme una autoritat o organisme públic,

b) les activitats principals del responsable o de l'encarregat consisteixin en operacions de tractament que, per raó de la seva naturalesa, del seu abast o de les seves finalitats, requereixen una observació habitual i sistemàtica d'interessats a gran escala, o

c) les activitats principals del responsable o de l'encarregat consisteixen en el tractament a gran escala de categories especials de dades personals, de conformitat amb l'article 9, i de les dades relatives a condemnes i infraccions penals a què es refereix l'article 10."

El delegat de protecció de dades s'ha de designar atenent a les seves qualitats professionals i, en particular, als coneixements especialitzats del dret, a la pràctica en matèria de protecció de dades i a la capacitat per a exercir les funcions indicades en l'article 39 (art. 37.5).

L'article 38 RGPD regula la posició del delegat de protecció de dades dins de l'administració, l'empresa o l'organització. En qualsevol cas, ha de garantir-se que participi en el moment oportú i de manera adequada en totes les qüestions relatives a la protecció de dades personals.

Així mateix, el RT i l'ET han de donar suport al delegat de protecció de dades en l'acompliment de les funcions i li han de facilitar els recursos necessaris per a l'acompliment de les seves responsabilitats i l'accés a les dades personals i a les operacions de tractament. Tant el responsable com l'encarregat s'han d'assegurar que el delegat no rep cap instrucció pel que fa a l'acompliment de les seves funcions, les duu a terme mantenint el secret i la confidencialitat i ret comptes al nivell jeràrquic més alt.

El delegat de protecció de dades té unes funcions mínimes, recollides en l'article 39.1 RGPD i que consisteixen a:

- Informar i assessorar el responsable o l'encarregat del tractament i els empleats de les obligacions que els incumbeixen (art. 39.1.a).

- Supervisar el compliment del que disposa el RGPD i altres disposicions de protecció de dades, així com de les polítiques del RT o ET en matèria de protecció de dades personals, inclosa l'assignació de responsabilitats, la conscienciació i la formació del personal que participa en les operacions de tractament i les auditories corresponents; (art. 39.1.b).

- Oferir l'assessorament que se li sol·licita sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar-ne l'aplicació (art. 39.1.c).

- Cooperar amb l'autoritat de control (art. 39.1.d).

- Actuar com a punt de contacte de l'autoritat de control per a qüestions relatives al tractament, inclosa la consulta prèvia, i fer consultes, si escau, sobre qualsevol altre assumpte (art. 39.1.e).

En l'acompliment de les seves funcions, el delegat haurà de fer-ho prestant l'atenció deguda als riscos associats a les operacions de tractament, tenint en compte la naturalesa, l'abast, el context i les finalitats del tractament (art. 39.2).

3.8. 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 representa 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 de *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 la correcta aplicació del RGPD.

Les **certificacions, segells i marques** ajuden a demostrar que s'està complint amb les disposicions del RGPD (es tracta, en definitiva, de mecanismes de *compliance*), això és, acrediten el compliment del RGPD.

Les organitzacions independents de certificació, ADP o bé el Comitè europeu de protecció de dades, han de certificar les empreses i dur a terme un seguiment del compliment adequat de la certificació. Això és, han de dur a terme un seguiment per a comprovar que l'empresa en qüestió compleix amb allò que ha estat certificat i s'hi adequa. Això també representa una novetat del RGPD respecte de la Directiva.

3.8.1. Els codis de conducta

Durant el procés d'adopció del RGPD es va posar de relleu el fet que l'aplicació del mateix podia suposar un cost elevat per a les PIMES. Un dels mecanismes per a respondre a aquesta crítica va ser la introducció de codis de conducta, que ja havien estat recollits en l'article 27 DPD, si bé havien passat una mica desapercebuts i no havien tingut massa joc en el marc de la Directiva.

Vegeu també

Els codis de conducta ja s'esmentaven en la DPD, si bé no se'ls va prestar gaire atenció.

Els codis de conducta constitueixen un mecanisme d'autoregulació (*self-regulatory instrument*). La seva eficàcia d'autoregulació depèn en part del nivell de ratificació que reben per part de les ADP o altres autoritats.

Actualment, amb l'excepció d'alguns sectors específics, hi ha pocs codis de conducta aprovats.

No obstant això, cada vegada es posa més de relleu el seu potencial per regular el tractament d'informació personal i cada vegada se'ls presta més atenció.

En essència, el compliment d'un codi de conducta pot ser seguit per una organització que té un nivell apropiat d'experiència en el sector concret que es tracta i està acreditat per a això (per a exercir aquesta funció) per l'autoritat competent.

Es considera que és una mesura adequada cap a l'autoregulació.

Segons disposa l'article 40.1 RGPD,

> "Els estats membres, les autoritats de control, el Comitè i la Comissió han de promoure l'elaboració de codis de conducta destinats a contribuir a l'aplicació correcta d'aquest RGPD. A aquest efecte han de tenir-se en compte les característiques específiques dels diferents sectors de tractament i les necessitats específiques de les microempreses i les petites i mitjanes empreses".

Les associacions i altres organismes representatius de categories de responsables o encarregats del tractament poden elaborar codis de conducta o modificar-los a fi d'especificar l'aplicació del RGPD pel que fa al següent:

El tractament lleial i transparent; els interessos legítims perseguits pels responsables del tractament en contextos específics; la recollida de dades personals; la seudonimització de dades personals; la informació proporcionada al públic i als interessats; l'exercici dels drets dels interessats; la informació proporcionada als nens i la protecció d'aquests, així com la manera d'obtenir el consentiment dels titulars de la pàtria potestat o de la tutela sobre el nen; les mesures i els procediments tècnics adequats, així com les mesures per a garantir la seguretat del tractament (art. 40.2 RGPD).

Així mateix, els responsables o els encarregats als quals no s'aplica aquest Reglament també poden adherir-se a codis de conducta que tinguin validesa general (art. 40.3 RGPD).

Els codis de conducta promoguts per les associacions i altres organismes representatius han de contenir mecanismes que permetin a l'organisme supervisor previst en l'article 41 RGPD efectuar el control obligatori del compliment de les seves disposicions pels responsables o encarregats de tractament que es comprometin a aplicar-lo, sense perjudici de les funcions i els poders de les autoritats de control que siguin competents (art. 40.4 RGPD).

Les associacions i altres organismes que projectin elaborar un codi de conducta o modificar o ampliar un codi existent han de presentar el projecte de codi o la modificació o ampliació a l'autoritat de control que sigui competent. L'autoritat de control ha de dictaminar si el projecte de codi o la modificació o ampliació és conforme a aquest Reglament i ha d'aprovar aquest projecte de codi o la modificació o ampliació si considera suficients les garanties adequades que ofereix (art. 40.5 RGPD).

Si el projecte de codi o la seva modificació o ampliació s'aprova i el codi de conducta de què es tracti no es refereix a activitats de tractament en diversos estats membres, l'autoritat de control ha de registrar i publicar el codi (art. 40.6 RGPD).

Si un projecte de codi de conducta té relació amb activitats de tractament en diversos estats membres, l'autoritat de control que sigui competent l'ha de presentar abans de la seva aprovació, o de la modificació o ampliació, al Comitè, el qual ha de dictaminar si aquest projecte, modificació o ampliació és conforme a aquest Reglament o si ofereix les garanties adequades (art. 40.7 RGPD).

Si el dictamen del Comitè confirma que el projecte, la modificació o l'ampliació del codi compleix el que disposa aquest Reglament o ofereix les garanties adequades, el Comitè ha de presentar el seu dictamen a la Comissió (art. 40.8 RGPD).

La Comissió, mitjançant actes d'execució, pot decidir que el codi de conducta o la modificació o l'ampliació que s'han aprovat i presentat tenen validesa general dins de la Unió (art. 40.9 RGPD).

La Comissió ha de donar publicitat adequada als codis aprovats la validesa general dels quals hagi estat decidida de conformitat amb l'article 40.9 RGPD (art. 40.10 RGPD).

El Comitè ha d'arxivar en un registre tots els codis de conducta, les modificacions i les ampliacions que s'aproven i posar-los a disposició pública per qualsevol mitjà apropiat (art. 40.11 RGPD).

Un element clau, respecte de l'adopció i la implementació dels codis de conducta és la seva supervisió. Aquesta l'ha d'efectuar un organisme extern al que tracta les dades personals i ha de complir amb una sèrie de requisits.

Sense perjudici de les funcions i els poders de l'autoritat de control competent, pot supervisar el compliment d'un codi de conducta un organisme que tingui el nivell adequat de perícia en relació amb l'objecte del codi i que hagi estat acreditat amb aquesta finalitat per l'autoritat de control competent (art. 41.1 RGPD).

A fi que un organisme pugui ser acreditat per a supervisar el compliment d'un codi de conducta han de complir-se una sèrie de requisits que preveu l'article 41.2 RGPD. Concretament que aquest organisme:

a) hagi demostrat la seva independència i perícia en relació amb l'objecte del codi;

b) hagi establert procediments que li permetin avaluar la idoneïtat dels responsables i els encarregats corresponents per aplicar el codi, supervisar el compliment de les seves disposicions i examinar periòdicament la seva aplicació;

c) hagi establert procediments i estructures per tractar les reclamacions relatives a infraccions del codi o a la manera en què el codi hagi estat o estigui sent aplicat per un responsable o encarregat del tractament, i per fer aquests procediments i estructures transparents per als interessats i el públic, i

d) hagi demostrat, a satisfacció de l'autoritat de control competent, que les seves funcions i tasques no donen lloc a conflicte d'interessos.

L'autoritat de control competent ha de sotmetre al Comitè, d'acord amb el mecanisme de coherència, el projecte que fixa els criteris d'acreditació d'un organisme supervisor (art. 41.3 RGPD).

Sense perjudici de les funcions i els poders de l'autoritat de control competent i del que disposa el capítol VIII, un organisme, amb subjecció a garanties adequades, ha de prendre les mesures oportunes en cas d'infracció del codi per un responsable o encarregat del tractament, inclosa la suspensió o l'exclusió d'aquest. Ha d'informar d'aquestes mesures i de les seves raons a l'autoritat de control competent (art. 41.4 RGPD).

Nota

El Capítol VIII del RGPD porta per rúbrica: "Recursos, responsabilitat i sancions".

L'autoritat de control competent ha de revocar l'acreditació d'un organisme si les condicions de l'acreditació no es compleixen o han deixat de complir-se, o si l'actuació d'aquest organisme infringeix aquest Reglament (art. 41.5 RGPD).

Ha de tenir-se en compte que la possibilitat de supervisar l'aplicació d'un codi de conducta per part d'un organisme extern, diferent d'una autoritat de control, no resulta aplicable al tractament realitzat per autoritats i organismes públics (art. 41.6 RGPD).

3.8.2. La certificació

La idea de la certificació té els orígens als EUA, que ja la va implementar des de 1990. A la UE han començat a adoptar-se si bé no tenen una ferma base ni teòrica ni legal. La filosofia a que responen a cada costat de l'Atlàntic és diferent.

Concretament, el model dels EUA és d'una autoregulació total. Per contra, en el marc del RGPD, es tracta d'un mecanisme establert sota l'escrutini directe/indirecte de la ADP competent.

El text originari de la Comissió proporcionava molta més iniciativa a aquesta, sobre la base del mecanisme de dictar actes delegats. El text final va optar per un model més concret. De manera que una certificació pot ser emesa per un ens certificador (sobre la base dels criteris adoptats per l'APD), o bé pot ser emesa per l'APD mateixa.

A aquests efectes s'estableix que

> "Els estats membres, les autoritats de control, el Comitè i la Comissió han de promoure, en particular en l'àmbit de la Unió, la creació de mecanismes de certificació en matèria de protecció de dades, i de segells i marques de protecció de dades a fi de demostrar el compliment del que disposa aquest Reglament sobre les operacions de tractament dels responsables i els encarregats. S'han de tenir en compte les necessitats específiques de les microempreses i les petites i mitjanes empreses" (art. 42.1 RGPD).

> "A més de l'adhesió dels responsables o dels encarregats del tractament subjectes a aquest Reglament, es poden establir mecanismes de certificació, segells o marques de protecció de dades aprovades de conformitat amb l'apartat 5, a fi de demostrar l'existència de garanties adequades ofertes pels responsables o encarregats no subjectes a aquest Reglament en el marc de transferències de dades personals a tercers països o organitzacions internacionals. Aquests responsables o encarregats han d'assumir compromisos vinculants i exigibles, per via contractual o mitjançant altres instruments jurídicament vinculants, per aplicar aquestes garanties adequades, incloses les relatives als drets dels interessats (art. 42.2 RGPD)".

La certificació és voluntària i ha d'estar disponible a través d'un procés transparent (art. 42.3 RGPD).

En qualsevol cas, la certificació no limita la responsabilitat del responsable o de l'encarregat del tractament quant al compliment del Reglament, i s'ha d'entendre 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 l'expedeixen els organismes de certificació esmentats en l'art. 43, o l'autoritat de control competent o el Comitè de conformitat amb l'article 63 (sobre la base dels mecanismes de coherència). Quan els criteris els aprova el Comitè, això pot donar lloc a una certificació comuna: el Segell Europeu de Protecció de Dades (art. 42.5 RGPD).

Els responsables o els encarregats que sotmetin el seu tractament al mecanisme de certificació han de donar a l'organisme de certificació o, si escau, a l'autoritat de control competent, tota la informació i accés a les seves activitats de tractament que necessiti per a dur a terme el procediment de certificació (art. 42.6 RGPD).

La certificació s'ha d'expedir a un responsable o encarregat de tractament per un període màxim de tres anys i es pot renovar en les mateixes condicions, sempre que se segueixin complint els requisits pertinents. La certificació serà retirada, quan escaigui, pels organismes de certificació o, si escau, per l'autoritat de control competent, quan no es compleixin o s'hagin deixat de complir els requisits per a la certificació (art. 42.7 RGPD).

El Comitè ha d'arxivar en un registre tots els mecanismes de certificació, els segells i les marques de protecció de dades i posar-los a disposició pública per qualsevol mitjà apropiat (art. 42.8 RGPD).

Aquest sistema de certificació es basa en l'existència d'uns organismes de certificació, que tinguin un nivell adequat de perícia i que han d'expedir i renovar les certificacions una vegada informada l'autoritat de control. En qualsevol cas ha de garantir-se que aquests organismes de certificació siguin acreditats per l'autoritat o l'organisme adequat.

Aquesta acreditació pot ser efectuada per una autoritat de control o per un organisme nacional d'acreditació (art. 43.1 RGPD).

Els organismes de certificació, per a poder ser acreditats, han de complir una sèrie de requisits (art. 43.2 RGPD).

Els organismes de certificació són responsables de la correcta avaluació a l'efecte de certificació o retirada de la certificació, sense perjudici de la responsabilitat del responsable o de l'encarregat del tractament quant al compliment d'aquest Reglament. L'acreditació s'ha d'expedir per un període màxim de cinc anys i es pot renovar en les mateixes condicions, sempre que l'organisme de certificació compleixi els requisits que estableix el RGPD (art. 43.4).

L'autoritat de control competent o l'organisme nacional d'acreditació ha de revocar l'acreditació a un organisme de certificació si les condicions de l'acreditació no es compleixen o han deixat de complir-se, o si l'actuació d'aquest organisme de certificació infringeix el RGPD (art. 43.7).

3.9. Drets de l'afectat/interessat

El capítol III del RGPDPD es dedica als drets de l'interessat. Aquest capítol es divideix en cinc seccions que fan referència a la 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 d'entrada que es recullen nous drets: el dret a la limitació del tractament i el dret a la portabilitat. Així mateix, el dret de cancel·lació passa a denominar-se *dret de supressió*. D'altra banda, el denominat *dret a l'oblit* s'esmenta en l'article 17 RGPD com un equivalent al dret de supressió i realment queda molt desnaturalitzat.

3.9.1. Transparència i modalitats

La secció 1 del capítol III porta per rúbrica "transparència i modalitats".

D'entrada ha de subratllar-se que el RGPD configura la transparència alhora com:

- Un principi de protecció de dades [art. 5.1.a) RGPD].Recordem que aquest precepte disposa el següent: 1. Les dades personals han de ser: a) tractades de manera lícita, lleial i transparent en relació amb l'interessat ("licitud, lleialtat i transparència").

- Un dret de les persones a rebre determinada informació.

Així mateix, la transparència estaria vinculada a l'exercici d'altres drets. És a dir, la informació que ha de proporcionar-se constitueix un pressupòsit per a poder exercir altres drets com el dret de rectificació, supressió, o bé oposar-se a tractaments que comportin decisions individuals automatitzades.

Per tant, en parlar de transparència es fa referència al fet que el tractament sigui lícit i lleial.

Article 12:Transparència de la informació, comunicació i modalitats d'exercici dels drets de l'interessat

L'article 12 fa referència a tres aspectes:

1) Referència general a la transparència. La referència a la transparència, a més de relacionar-la amb l'article 5.1.a) RGPD, ha de posar-se en relació amb el principi de responsabilitat proactiva (art. 5.2 RGPD), de manera que el RT ha d'actuar de forma diligent i proporcionar tots els mecanismes (entre ells la informació necessària) per a fer efectius els drets de l'afectat.

2) Forma de comunicació. La comunicació a l'interessat ha de fer-se "de manera concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill, en particular qualsevol informació dirigida específicament a un nen" (art. 12.1 RGPD). La informació s'ha de donar per escrit o per altres mitjans, inclososels mitjans electrònics. Si ho sol·licita l'interessat també es pot donar verbalment, si es demostra la identitat de l'interessat (art. 12.1 RGPD).

El RT ha de donar a l'interessat la informació relativa a les seves actuacions sobre la base de 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-se dos mesos més en cas necessari, i ha d'informar-se l'interessat d'aquestes pròrrogues (art. 12.3 RGPD).

La informació facilitada ha de ser gratuïta. Això no obstant,si les peticions són manifestament infundades o excessives (pel seu caràcter repetitiu), el RT pot cobrar un cànon raonable o bé negar-se a actuar respecte de la sol·licitud (art. 12.5 RGPD).

Un aspecte important és la previsió de la possibilitat que la informació que hagi de facilitar-se als interessats es faci en combinació amb icones normalitzades que permetin proporcionar de forma fàcilment visible, intel·ligible i clarament llegible una visió de conjunt adequada del tractament previst (art. 12.7 RGPD). Aquesta iniciativa ja s'ha proposat en ocasions anteriors, i en tot cas la seva implementació es deixa a la Comissió (art. 12.8 RGPD). D'alguna manera es vol incorporar les imatges visuals dels *creative commons*, de manera que sigui clarament identificable per als afectats.

3) Modalitats d'exercici dels drets per part de l'interessat.

3.9.2. Informació i accés a les dades personals

La secció 2 del capítol III es dedica a la informació i accés a les dades personals.

Quant al contingut concret de la informació que ha de proporcionar-se a l'interessat/afectat, el RGPD, igual que la DPD, el 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 al següent:

- L'àmbit subjectiu: qui és el responsable del tractament i el delegat de protecció de dades;així com els destinataris o categories de destinataris de les dades i la intenció de transferir les dades a un tercer país o organització internacional.

- Quant al contingut concret, un aspecte rellevant és proporcionar informació de les finalitats del tractament i la seva base jurídica. Una novetat és que, en els casos en què la base jurídica sigui l'interès legítim (art. 6.1.f), ha d'especificar-se quin és aquest (art. 13.1.d RGPD).

Així mateix, segons disposa l'article 13.2, ha de proporcionar-se informació relativa al següent:

- El termini durant el qual es conserven les dades personals i, si això no és possible, els criteris utilitzats per a determinar aquest termini.

- L'existència dels drets que té l'afectat (accés, rectificació, supressió, limitació, oposició i portabilitat).

- L'existència del dret a revocar el consentiment (el text del RGPD fa referència a "retirar" el consentiment si bé el terme més apropiat és el de *revocar*).

- El dret a presentar una reclamació davant l'autoritat competent.

- El caràcter obligatori o no de facilitar les dades.

- Un aspecte de gran transcendència és la necessitat de comunicar l'existència de decisions automatitzades, inclosa l'elaboració de perfils (art. 22 RGPD), així com informació significativa sobre la lògica aplicada i les conseqüències previstes d'aquest tractament per a l'interessat. Això és ha de proporcionar-se informació específica relativa a les decisions automatitzades [vinya art. 13.1. (f)].

Segons estableix l'article 13.3, en els supòsits en què el RT projecti el tractament ulterior de dades per a una finalitat que no sigui aquella per la qual es van recollir, abans d'aquest tractament ha de proporcionar a l'interessat informació sobre aquesta altra finalitat (vegeu també l'art. 6.4 RGPD).

Aquesta informació ha de facilitar-se a l'interessat en el moment en què s'obtinguin les dades (art. 13.1).

En els supòsits en què l'interessat ja disposi de la informació prevista, no cal proporcionar-la-hi (art. 13.4 RGPD).

Supòsits en què les dades no s'obtenen directament de l'afectat. A part d'alguns aspectes que són similars als del punt anterior, en aquest cas hi ha aspectes nous (vegeu l'art. 13 RGPD).

Aquest és el cas de l'art. 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;

En canvi, no cal proporcionar informació sobre el següent:

El que disposa l'article 13.2.e) RGPD si la comunicació de dades personals és un requisit legal o contractual, o un requisit necessari per a subscriure un contracte, i si l'interessat està obligat a facilitar les dades personals i està informat de les possibles conseqüències de no facilitar aquestes dades; això és obvi, perquè en aquest cas les dades no les proporciona l'afectat (no se sol·liciten d'ell), sinó que s'obtenen d'una altra font o d'un tercer.

D'altra banda, en la mesura que les dades no s'obtenen de l'afectat, és important determinar en quin moment se li ha de proporcionar la informació. L'article 14.3 estableix diferents supòsits:

La regla general és la d'un termini raonable, una vegada obtingudes les dades, i com a màxim dins d'un mes segons les circumstàncies en les quals es tractin les dades.

En els casos en què les dades s'utilitzin per a comunicar-se amb l'interessat, com a màxim en el moment de la primera comunicació a aquest interessat. Si es comuniquen a un altre destinatari, com a molt tard en el moment en què les dades personals siguin comunicades per primera vegada.

La norma també preveu supòsits en què no cal proporcionar la informació a l'afectat:

- Si l'interessat ja disposa de la informació.

- Quan la comunicació resulti impossible o impliqui un esforç. desproporcionat, especialment amb finalitats d'arxiu en interès públic, finalitats de recerca científicai històrica o finalitats estadístiques. Tanmateix, en aquest cas, ha de complir-se amb les garanties de l'article 89 RGPD. En aquests casos el RT ha d'adoptar les mesures adequades per a protegir els drets, llibertats i interessos legítims de l'interessat, fins i tot fent pública la informació (art. 14.5.b) RGPD).

- L'obtenció o comunicació està expressament establerta per la legislació.

- Quan les dades personals hagin de seguir tenint caràcter confidencial, sobre la base d'una obligació de secret professional, regulada en el dret de la Unió o dels estats membres, inclosa una obligació de secret de naturalesa estatutària.

Estretament lligat a la informació hi ha l'aspecte de l'accés a aquesta, 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 del responsable del tractament confirmació de si s'estan tractant 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 (art. 15.1 RGPD).

La informació a la qual es té accés és la relativa al següent:

- les finalitats del tractament;

- les categories de dades personals que es tracten;

- els destinataris o les categories de destinataris de les dades; el termini previst de conservació de les dades personals o els criteris utilitzats per a determinar aquest termini;

- l'existència dels drets que corresponen a l'afectat; el dret a presentar una reclamació davant una autoritat de control; quan les dades personals no s'hagin obtingut de l'interessat, qualsevol informació disponible sobre el seu origen; l'existència de decisions automatitzades, inclosa l'elaboració de

perfils i en aquests casos, informació significativa sobre la lògica aplicada, així com les conseqüències previstes d'aquest tractament per a l'interessat.

En els casos en què es transfereixin dades a un tercer país o una organització internacional, l'interessat té dret a ser informat de les garanties adequades.

Un aspecte nou del RGPD és que es determina que el RT ha de facilitar una còpia de les dades personals. Fins ara, la pràctica del dret d'accés no s'exercia proporcionant accés directe a les dades, per la qual cosa això exigeix un canvi en la modalitat de l'exercici d'aquest dret (art. 15.3 RGPD). En els casos en què se sol·licitin còpies ulteriors es pot percebre un cànon raonable per això.Si la sol·licitud es presenta per mitjans electrònics, i tret que l'interessat sol·liciti que es faciliti d'una altra manera, la informació s'ha de facilitar en un format electrònic d'ús comú (art. 15.3 RGPD).

En qualsevol cas, el dret a obtenir còpia no ha d'afectar negativament els drets i llibertats d'altres subjectes (art. 15.4 RGPD).

3.9.3. Rectificació i supressió

La secció 3 del capítol III porta per rúbrica "Rectificació i supressió". Com ja s'ha indicat, en la nova regulació, la referència al dret de cancel·lació ha estat substituïda per la de supressió.

Article 16: Dret de rectificació

L'interessat té dret a obtenir sense dilació indeguda del responsable del tractament la rectificació de les dades personals inexactes que l'afecten. Tenint en compte les finalitats del tractament, l'interessat té dret que es completin les dades personals que siguin incompletes, fins i tot mitjançant una declaració addicional.

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

L'expressió"sense dilació indeguda" no sembla que hagi d'entendre's com si el termini fos diferent del previst de forma general per a l'exercici dels altres drets, això és, d'1 mes.

Així mateix, en els supòsits en què es procedeix a la rectificació, ha de comunicar-se als destinataris que aquesta rectificació ha tingut lloc, tret que això sigui impossible o impliqui un esforç desproporcionat. Així mateix l'afectat també té dret a saber qui ha estat el destinatari de les dades.

Article 17: Dret de supressió ("el dret a l'oblit")

1) L'interessat té dret a obtenir sense dilació indeguda del responsable del tractament la supressió de les dades personals que l'afecten, el qual està obligat a suprimir sense dilació indeguda les dades personals quan concorri alguna de les circumstàncies següents:

a) Les dades personals ja no són necessàries en relació amb les finalitats per a les quals van ser recollides o tractades.

b) L'interessat retira el consentiment en què es basa el tractament (es tracta del supòsit de la revocació del consentiment).

c) L'interessat s'oposa al tractament i no prevalen altres motius legítims per a aquest.

d) Les dades personals han estat tractades il·lícitament.

e) Les dades personals han de suprimir-se per al compliment d'una obligació legal establerta en el dret de la Unió o dels estats membres.

f) Les dades personals s'han obtingut en relació amb l'oferta de serveis de la societat de la informació esmentats en l'article 8, apartat 1 (es tracta de l'oferta realitzada a nens, entesos aquests com a menors de 18 anys).

L'article 17.2 disposa que en els casos en què el RT hagi fet públiques les dades personals i en virtut de l'article 17.1 RGPD estigui obligat a suprimir aquestes dades, el RT, tenint en compte la tecnologia disponible i el cost de la seva aplicació, ha d'adoptar mesures raonables, incloses mesures tècniques, amb la intenció d'informar els responsables que estiguin tractant les dades personals de la sol·licitud de l'interessat de supressió de qualsevol enllaç a aquestes dades personals, o qualsevol còpia o rèplica d'aquestes.

Per tant, el RT inicial, ha d'adoptar mesures raonables per a comunicar a ulteriors RT de la sol·licitud de l'afectat de voler suprimir qualsevol enllaç a les dades personals. Es tracta d'una obligació de mitjans, de manera que el RT inicial no ha d'assegurar en tot cas que els destinataris de les dades (els altres RT) les deixen de tractar, sinó que empra els mitjans dels que disposa per dur a terme aquesta comunicació.

Tanmateix,l'article 17.3 estableix supòsits en què aquesta aplicació del dret a eliminar dades i enllaços no resulta aplicable. Concretament, en els casos en què la permanència d'aquestsés necessària:

1) per a exercir el dret a la llibertat d'expressió i informació;

2) per al compliment d'una obligació legal que requereixi el tractament de dades o per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable;

3) per raons d'interès públic en l'àmbit de la salut pública;

4) amb finalitats d'arxiu en interès públic, finalitats de recerca científica o històrica o finalitats estadístiques, de conformitat amb l'article 89, apartat 1;

5) per a la formulació, l'exercici o la defensa de reclamacions.

Què ha quedat del denominat dret a l'oblit?

La mesura que recull l'article 17.2 RGPD tracta d'evitar multiplicar els efectes de rèplica dels enllaços successius de la informació.

A pesar que la rúbrica de l'article 17 fa referència entre parèntesis al dret a l'oblit, se'n fa una referència confusa. De fet, la utilització d'aquesta terminologia no és més que un arrossegament dels textos anteriors a l'aprovació del RGPD. El denominat *dret a l'oblit*, tal com es troba regulat en el RGPD, no és tal, sinó que és una manifestació dels drets d'oposició i cancel·lació. Les característiques i requisits del dret a l'oblit es troben a la STJUE, en el cas Google Spain, S.L., Google Inc. v. Agència Espanyola de Protecció de Dades (AEPD) i Mario Costeja González (C 131/12), de 13 de maig de 2014.

> En lloc de fer referència al dret a l'oblit sembla més correcte parlar del dret a ser eliminat de la llista de resultats dels motors de cerca (*right to be delisted*). En rigor, el que l'afectat pot sol·licitar és que al dur-se a terme recerques a internet en base al seu nom, deixi d'aparèixer en els resultats que ofereix el motor de cerca. Aquesta petició té possibilitats de prosperar si la informació és totalment irrellevant i obsoleta. El motor de cerca (no l'editor de la informació) porta a terme una ponderació dels drets implicats (el de l'afectat vs el dret del públic a obtenir informació). En tot cas l'interessat sempre podrà acudir a l'APD i a l'autoritat judicial. No obstant això, en cas de prosperar la petició de ser eliminat de la llista de resultats, la informació roman en la seva font original (l'hemeroteca d'un diari o un butlletí oficial).

Segons disposa l'article 17.2 RGPD, quan el RT faci públiques les dades i tingui l'obligació de suprimir-les, aquest RT té l'obligació d'informar el tercer responsable de la sol·licitud de l'interessat de supressió de qualsevol enllaç a les dades.

Es tracta d'una obligació d'informar els tercers, en funció dels mitjans de què disposi el RT (de la tecnologia i dels costos) i és obligació de mitjans (no de resultat).

Article 18: Dret a la limitació del tractament

1) Com s'ha indicat, es tracta d'un nou dret en virtut del qual l'interessat té dret a obtenir del responsable del tractament la limitació del tractament de les dades quan es compleixin determinades condicions:

a) l'interessat impugna l'exactitud de les dades personals, durant un termini que permet al responsable verificar-ne l'exactitud;

b) el tractament és il·lícit i l'interessat s'oposa a la supressió de les dades personals i sol·licita, en el seu lloc, la limitació del seu ús;

c) el responsable ja no necessita les dades personals per a les finalitats del tractament, però l'interessat les necessita per a formular, exercir o defensar reclamacions;

d) l'interessat s'ha oposat al tractament en virtut de l'article 21, apartat 1, mentre es verifica si els motius legítims del responsable prevalen sobre els de l'interessat.

2) Quan el tractament de dades personals s'ha limitat en virtut de l'apartat 1, aquestes dades solament es poden tractar, amb excepció de la seva conservació, amb el consentiment de l'interessat o per a formular, exercir o defensar reclamacions, o amb la intenció de protegir els drets d'una altra persona física o jurídica, o per raons d'interès públic important de la Unió o d'un determinat estat membre.

3) Qualsevol interessat que hagi obtingut la limitació del tractament d'acord amb l'apartat 1 ha de ser informat pel responsable abans de l'aixecament d'aquesta limitació.

Es tracta d'un nou dret de conseqüències importants. La diferència principal respecte del bloqueig de les dades és que no es tracta d'una obligació sinó d'un dret de l'interessat.

Es distingeix un ventall de supòsits. Uns són equivalents a la cancel·lació cautelar (cf. impugnar exactitud de dades), si bé cautelarment han de conservar-se. També si l'interessat exerceix el dret d'oposició de l'exarticle 21.1 mentre se'n verifica la procedència.

Es produeix una inversió de la càrrega de la prova de manera que quan el RT al·legui un interès (públic, o legítim) haurà de demostrar-lo. Un altre supòsit és el que respon a la voluntat de l'afectat, per exemple, perquè l'interessat pugui obtenir determinades proves.

Quines són les conseqüències de la limitació del tractament? Segons l'art. 18.2 RGPD, les conseqüències són que el tractament es limita a la conservació de les dades, tret que es donin diferents supòsits. L'article 19 també disposa la necessitat de comunicar-lo als destinataris de la comunicació.

Es reforça aquest dret de manera que, abans d'aixecar la limitació, el RT ha d'informar l'afectat. No pot aixecar-se la limitació sense que l'afectat ho sàpiga (art. 18.3 RGPDPD). També ha de proporcionar-se informació sobre els destinataris de la informació (art. 19.3 RGPDPD).

Per a fer efectius els drets de rectificació, supressió i limitació del tractament, s'habiliten una sèrie de mesures especialment quan les dades s'han transmès a tercers. Segons disposa l'article 19 RGPD, el RT ha de comunicar qualsevol rectificació o supressió de dades personals o limitació del tractament efectuada a cadascun dels destinataris als quals s'hagin comunicat les dades personals, tret que sigui impossible o exigeixi un esforç desproporcionat.

Així mateix el RT ha d'informar l'interessat sobre aquests destinataris, si aquest ho sol·licita.

Article 20: el dret a la portabilitat de les dades

Una altra mesura rellevant és el dret a la portabilitat de les dades recollida en l'article 20.

1) L'interessat té dret a rebre les dades personals que l'afecten, que hagi facilitat a un responsable del tractament, en un format estructurat, d'ús comú i lectura mecànica, i a transmetre-les a un altre responsable del tractament sense que ho impedeixi el responsable al qualles havia facilitat, quan:

a) el tractament estigui basat en el consentiment o en un contracte i

b) el tractament s'efectuï per mitjans automatitzats.

2) En exercir el dret a la portabilitat de les dades (exart. 20.1), l'interessat té dret al fet que les dades personals es transmetin directament de responsable a responsable quan sigui tècnicament possible.

3) L'exercici del dret esmentat en l'apartat 1 d'aquest article s'entén sense perjudici de l'article 17. Aquest dret no s'aplica al tractament que sigui necessari per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament.

El dret a la portabilitat no ha d'afectar negativament els drets i llibertats dels altres (art. 20.4 RGPD).

Es tracta d'una novetat important, com un complement del tradicional dret d'accés. Es tracta del dret de rebre les dades que afecten un interessat/afectat.

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

Què ha d'entendre's per "dades que l'afectat ha facilitat a un RT"? Això pot ser discutible. Es considera que les dades no han de limitar-se a les que han estat facilitades per l'afectat, sinó que també n'hi ha d'altres. Per exemple, aquelles en què l'activitat amb l'interessat dóna lloc a un tractament de dades, com ara dades de navegació de l'interessat.

Cal pensar no solament en les dades facilitades pel mateix afectat, sinó tambéen les que s'obtenen de forma indirecta. Això no obstant, els tractaments addicionals que pugui fer el RT no són objecte de portabilitat.

Un altre aspecte important és el dret a transmetre les dades a un altre RT sense que ho impedeixi el RT inicial. Es tracta, doncs, d'un dret molt adequat a la prestació de serveis a internet, especialment en el cas de les xarxes socials.

Lògicament, és impensable que cada interessat tingui la capacitat i la tecnologia suficients per a poder desar i migrar les dades. En conseqüència, l'efectivitat del dret quedaria menyscabada. Per això és una mesura molt positiva que s'estableixi que les dades poden transmetre's a un altre RT.

Perquè es pugui aplicar aquest dret cal que la base del tractament sigui molt concreta.

Quant a la modalitat d'exercici d'aquest dret, ja s'ha indicat que és possible la transmissió de les dades a un tercer, de manera que s'estimula el desenvolupament de sistemes interoperables en la prestació del servei.

Lògicament, també hi ha limitacions a aquest dret, quan hi ha una base jurídica diferent que habilita el RT a seguir conservant les dades o bé quan el fonament de la conservació es basa en una obligació legal.

3.9.4. Dret d'oposició i decisions individuals automatitzades

La secció 4 del capítol III porta per rúbrica "Dret d'oposició i decisions individuals automatitzades".

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

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. L'article 6.1.e) és aquell en què el tractament és necessari per al compliment d'una missió realitzada en interès públic o en l'exercici de

poders públics conferits al responsable del tractament. L'article 6.1.f) habilita el tractament quan és necessari per a la satisfacció d'interessos legítims perseguits pel responsable del tractament.

En aquests casos, l'interessat té dret a oposar-se en qualsevol moment al tractament al·legant una situació particular.

La petició de l'afectat ha de motivar-se. Si preval l'exercici del dret d'oposició, el RT ha de deixar de tractar les dades tret que acrediti que hi ha motius legítims imperiosos per al tractament que prevalguin sobre els interessos, els drets i les llibertats de l'interessat o bé per a la formulació, l'exercici o la defensa de reclamacions.

L'AEPD admet un concepte ampli i flexible de l'exigència de motivació.

L'article 21.2 preveu l'exercici del dret d'oposició quan el tractament de dades personals té 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 l'afecten, inclosa l'elaboració de perfils en la mesura en què estigui relacionada amb el màrqueting esmentat. En aquest cas, les dades personals han de deixar de ser tractades per a aquestes finalitats (art. 21.3). Es tracta d'un supòsit d'*opt-out* immotivat, l'afectat pot oposar-s'hi en qualsevol moment.

Com a màxim en la primera comunicació que es realitzi amb l'interessat, se l'ha d'informar del dret d'oposició, ex art. 21.1 i 21.2 (art. 21.4 RGPD).

Quant al tractament de dades personals amb finalitats de recerca científica o històrica o finalitats estadístiques (exart. 89.1 RGPD), l'interessat, per motius relacionats amb la seva situació particular, té dret a oposar-se al tractament de dades personals que l'afectin, tret que sigui necessari per al compliment d'una missió duta a terme per raons d'interès públic (art. 21.6 RGPD).

Juntament amb aquesta regla general continguda en l'article 21 RGPD, existeix legislació específica en què hi ha la possibilitat d'exercir el dret d'oposició. Per exemple, en la legislació sobre telecomunicacions o bé en el marc de la LSSI. Per exemple, el dret a no rebre trucades telefòniques que no són automàtiques.

En altres casos, més que l'exercici del dret d'oposició, el que es produeix és una revocació del consentiment atorgat (art. 7.3 RGPD). Això pot donar-se en els supòsits en què el fonament legal del tractament és el consentiment de l'afectat [art. 6.1.a) o bé art. 9.2.a) RGPD].

L'article 22 RGPD fa referència a les **decisions individuals automatitzades i a l'elaboració de perfils**.

D'entrada cal tenir en compte l'article. 4.4 RGPD, que proporciona una definició del que es considera "elaboració de perfils". S'entén com a tal

> "tota forma de tractament automatitzat de dades personals consistent a utilitzar 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 forma automàtica, sense intervenció humana. Sobre la base 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 aparentment hi hagi 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 qualsevol interessat té dret a no ser objecte d'una decisió basada únicament en el tractament automatitzat, inclosa l'elaboració de perfils, que produeixi efectes jurídics en ell o l'afecti significativament de manera similar (art. 22.1 RGPD).

Això no obstant, aquest dret també reconeix algunes excepcions (art. 22.3 RGPD), de manera que la previsió general no és aplicable si la decisió:

a) és necessària per a la subscripció o l'execució d'un contracte entre l'interessat i un responsable del tractament;

b) està autoritzada pel dret de la Unió o dels estats membres que s'apliqui al responsable del tractament i que estableixi així mateix mesures adequades per a salvaguardar els drets i llibertats i els interessos legítims de l'interessat, o

c) es basa en el consentiment explícit de l'interessat.

En els casos a què es refereix l'apartat 2, lletres *a* i *c*, el responsable del tractament ha d'adoptar les mesures adequades per a salvaguardar els drets i llibertats i els interessos legítims de l'interessat, com a mínim el dret a obtenir intervenció humana per part del responsable, a expressar el seu punt de vista i a impugnar la decisió (vegeul'art. 22.3 RGPD).

Així mateix, com a regla general, les decisions automatitzades no s'han de basar en les categories especials de dades personals que preveu l'article 9, apartat 1, això és, les denominades *dades sensibles* (vegeu l'art. 22.4 RGPD).

Quant a la valoració general del precepte, ha de recordar-se que no es tracta solament de drets, sinó també de garanties per a poder predicar l'existència d'un tractament lleial i transparent i que es compleixen els principis bàsics del RGPD. En definitiva, es tracta de corregir elements que poden generar inexactituds i reduir els riscos d'error.

3.9.5. Limitacions

La secció 5 del capítol III porta per rúbrica "Limitacions".

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

L'article 23.1 RGPD estableix que:

> "El dret de la Unió o dels estats membres que s'aplica al responsable o l'encarregat del tractament pot limitar, amb mesures legislatives, l'abast de les obligacions i dels drets que estableixen els articles 12 a 22 i l'article 34, així com l'article 5 en la mesura en què les seves disposicions es corresponguin amb els drets i les obligacions que preveuen els articles 12 a 22, quan aquesta limitació respecti en l'essencial els drets i les llibertats fonamentals i sigui una mesura necessària i proporcionada en una societat democràtica pera
>
> salvaguardar (entre altres): a) la seguretat de l'Estat; b) la defensa; c) la seguretat pública; d) la prevenció, investigació, detecció o enjudiciament d'infraccions penals, o l'execució de sancions penals, e) altres objectius importants d'interès públic; f) la protecció de la independència judicial i dels procediments judicials; g) la prevenció, la investigació, la detecció i l'enjudiciament d'infraccions de normes deontològiques; h) una funció de supervisió, inspecció o reglamentació; i) la protecció de l'interessat o dels drets i llibertats d'altres; j) l'execució de demandes civils.
>
> Això no obstant, les mesures legislatives adoptades han d'especificar, entre altres qüestions(art. 23.2.c), les garanties per a evitar accessos o transferències il·lícits o abusius; f) els terminis de conservació i les garanties aplicables tenint en compte la naturalesa,l'abast i els objectius del tractament o les categories de tractament; g) els riscos per als drets i les llibertats dels interessats, i h) el dret dels interessats a ser informats sobre la limitació."

En l'enumeració de les limitacions, la majoria són les tradicionals, si bé se n'inclouen algunes de noves com les relatives a motius econòmics financers, sanitat pública, protecció i independència judicial.

S'exigeixen garanties complementàries en relació amb la finalitat, les categories de dades. Així mateix, en aquest supòsit, les mesures de seguretat tenen un paper molt rellevant. I tots aquests aspectes es tenen en compte sobre la base dels riscos que poden amenaçar les dades dels afectats.

3.10. Transferències internacionals de dades

El capítol V RGPD es dedica a les transferències internacionals de dades i porta per rúbrica: "Transferències de dades personals a tercers països o organitzacions internacionals".

Es considera que hi ha una transferència de dades quan un RT o ET que està a la UE transmet dades a un RT o un altre subjecte que es troba fora de la UE. Per tant, les comunicacions de dades entre subjectes que es troben al territori de la UE no es consideren una transferència internacional de dades i no hi ha limitacions per a aquestes. De fet, un dels objectius de la D 95/46 era precisament el de facilitar la circulació de les dades entre els països de la Unió.

Tal com disposa l'article 44 RGPD, les transferències internacionals tenen com a destinataris "tercers països o bé organitzacions internacionals".

La regulació que proporciona el RGPD de les transferències internacionals no planteja novetats substancials respecte del règim contingut en la DPD. La idea que presideix el règim legal actual és que quan les dades surtin de la UE se segueixi aplicant el mateix nivell de protecció que gaudien en la UE. Això és, que quan les dades s'exportin, no disminueixin les garanties dels subjectes interessats. Així ho disposa, entre altres, l'article 44 RGPD, que disposa:

> "Totes les disposicions d'aquest capítol s'han d'aplicar a fi d'assegurar que el nivell de protecció de les persones físiques garantit per aquest Reglament no es vegi menyscabat".

El model és, doncs, que el de continuïtat del nivell de protecció.La normativa tracta d'obtenir i perseguir que el nivell de protecció garantit per la normativa europea es mantingui allà on es trobin les dades.

Les transferències internacionals de dades solament es basen en tres possibles fonaments, de manera que les transferències poden tenir lloc si:

1) Hi ha una decisió d'adequació (art. 45 RGPD).Es tractaria del nivell bàsic que tracta d'assegurar un nivell de protecció adequat respecte d'un territori concret, mitjançant l'adopció d'una declaració d'adequació. Quan existeix aquesta decisió significa s'ha produït l'anàlisi conforme el qual la destinació de les dades (territori, país) ofereix un nivell de protecció adequat. Nivell de protecció adequat al que s'estableix a la UE.

2) A falta de decisió d'adequació, solament poden transmetre's dades personals a un tercer país o organització internacional si s'ofereixen garanties adequades i a condició que els interessats disposin de drets exigibles i d'accions legals efectives (art. 46 RGPD).

3) En els casos en què no hi hagi un nivell de protecció adequat, ni tampoc s'hagin pogut donar garanties suficients, s'entra dins dels supòsits d'excepcions. Es poden transferir les dades si concorren una sèrie d'excepcions, i això obeeix a un interès de més valor, de millor qualitat.

Per tant, en primer lloc, es busca l'adequació del nivell de protecció d'un país o territori a les exigències de protecció que planteja la UE. A falta d'aquesta declaració d'adequació, es busca l'adopció de garanties suficients que en aquest

cas s'atorguen respecte d'un àmbit concret o bé d'una organització. A falta d'aquest atorgament entren en joc les excepcions que permeten les transferències internacionals de dades.

3.10.1. Novetats principals del règim de transferència de dades

L'objectiu de la Comissió i dels colegisladors en regular les transferències de dades era introduir més flexibilitat en aquest règim, que es criticava per ser excessivament burocratitzat. Així mateix, també es qüestionava el model existent d'adequació, en la mesura que hi havia poques declaracions i les que hi havia eren molt heterogènies.

D'altra banda, ha de tenir-se en compte que les transferències internacionals no són l'excepció, sinó que s'han convertit en la regla general. Pel que fa a les principals novetats cal destacar:

1) Referència al fet que l'exportador pot ser tant el RT com l'ET. En alguns països ja es feia aquesta equiparació, com per exemple en el marc de la LOPD. En canvi, en altres països només podien adoptar la decisió d'enviar dades fora de la UE els RT. Així mateix, les garanties poden proporcionar-les tant el RT com l'ET.

2) Les transferències poden fer referència tant a un país com a una organització internacional. La DPD solament feia referència a països o territoris, no a OI. En la pràctica, les transferències a aquestes OI són freqüents. Aquestes poden ser intergovernamentals o privades.

3) Per primera vegada, es dóna cabuda a les normes corporatives vinculants (conegudes també per les seves sigles en anglès: BCR, *binding corporate rules*). Es tracta d'una construcció desenvolupada per la pràctica i pel Grup de l'article 29, que havia fixat un conjunt de requisits per a la seva implementació, però no havien rebut suport legal. El RGPD les recull i les regula detalladament.

3.10.2. Transferències basades en una decisió d'adequació

Segons disposa l'article. 45.1 RGPD

> "Pot fer-se una transferència de dades personals a un tercer país o organització internacional quan la Comissió 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. Aquesta transferència no requereix cap autorització específica".

La decisió l'adopta la Comissió, mitjançant un procediment normatiu propi, i en aquest procés són consultades les APD a través de l'òrgan que les agrupa i que constitueix el Comitè europeu de protecció de dades.

Segons disposa l'article 45.2 RGPD, en avaluar l'adequació del nivell de protecció, la Comissió ha de tenir en compte, en particular, els elements següents:

- L'estat de dret, el respecte dels drets humans i les llibertats fonamentals i la legislació pertinent.

- L'existència i el funcionament efectiu d'una o diverses autoritats de control independents al tercer país.

- Els compromisos internacionals assumits pel tercer país o organització internacional de què es tracti.

La Comissió, després d'haver avaluat l'adequació del nivell de protecció, podrà decidir que un tercer país, un territori o un o diversos sectors específics d'un tercer país, o una organització internacional garanteixen un nivell de protecció adequat. Un aspecte important és que s'han d'establir mecanismes de revisió periòdica, almenys cada quatre anys, que tinguin en compte tots els esdeveniments rellevants al tercer país o en l'organització internacional, per a decidir si es manté o no la decisió d'adequació (art. 45.3. RGPD).

En conseqüència, en els casos en què es mostri que el lloc de destinació de les dades no garanteix un nivell de protecció adequat, la Comissió ha de derogar, modificar o suspendre sense efecte retroactiu la decisió d'adequació (art. 45.5).

La Comissió ha de fer pública la informació relativa als territoris, sectors o organitzacions internacionals que tenen un nivell de protecció adequat i als que l'han deixat de tenir (art. 45.8 RGPD).

Segons disposa l'article 45.9. RGPD, les decisions d'adequació ja adoptades han de seguir en vigor mentre la Comissió no les substitueixi, modifiqui o derogui.

En definitiva, el rellevant és que la Comissió, una vegada presa la decisió d'adequació, ha de seguir supervisant i monitorant la situació en les destinacions que es declaren de protecció adequada.

Aquest seguiment ha d'interpretar-se tenint en compte la STJUE, com per exemple en el cas *Schrems*, en què el TJUE va considerar que el concepte d'*adequació* ha d'interpretar-se com un concepte de protecció essencialment equivalent i que la Comissió ha de supervisar diligentment les condicions existents als països que es declaren adequats.

Cas *Schrems*

Es tracta de la STJUE de 6 d'octubre de 2015, C-362/14, Schrems.

3.10.3. Transferències basades en garanties adequades

L'article 46.1 determina que

"A falta de decisió d'acord amb l'article 45, apartat 3, el responsable o l'encarregat del tractament solament pot transmetre dades personals a un tercer país o organització internacional si ha ofert garanties adequades i a condició que els interessats disposin de drets exigibles i accions legals efectives."

Quant a les garanties adequades, han de distingir-se dos supòsits:

1) Garanties adequades que no necessiten autorització prèvia. Es tracta de les garanties recollides en l'article 46.2 RGPD que poden ser aportades, sense que es requereixi cap autorització expressa d'una autoritat de control, mitjançant:

a) Instruments jurídicament vinculants i executables entre autoritats o organismes públics.

b) Normes corporatives vinculants (BCR) art. 47 RGPD, tant respecte al RT com respecte a l'ET.

c) Clàusules contractuals estàndard aprovades per la Comissió.

d) Clàusules contractuals estàndard aprovades per una APD nacional i acceptades per la Comissió.

e) Codis de conducta i esquemes de certificació, que incloguin compromisos vinculants i executables per part del RT o l'ET al tercer país a fi de garantir suficientment la tutela dels drets de l'interessat.

En els supòsits previstos en l'article 46.2 RGPD, el fet que no calgui autorització prèvia comporta que puguin efectuar-se transferències emparant-se en clàusules generals o BCR sense haver de demanar autorització en cada cas. D'aquesta manera, si hi ha una BCR, pot dur-se a terme una transferència sense haver de demanar autorització prèvia. Una vegada la BCR està aprovada, poden dur-se a terme transferències de dades a l'empara d'aquesta.

Les BCR es regulen detalladament en l'article 47 RGPD. Segons disposa l'article 47.1 RGPD, l'autoritat de control competent ha d'aprovar normes corporatives vinculants d'acord amb el mecanisme de coherència establert en l'article 63, sempre que aquestes:

- Siguin jurídicament vinculants i s'apliquin i siguin complertes per tots els membres del grup empresarial o unió d'empreses.

- Confereixin expressament als interessats drets exigibles en relació amb el tractament de les seves dades personals.

- Incloguin els aspectes que preveu l'article. 47.2 RGPD.

Entre els aspectes que han d'incloure les BCR (recollits en l'art. 47.2 RGPD) destaquen:

L'estructura i les dades de contacte del grup empresarial o de la unió d'empreses i de cadascun dels seus membres.

Transferències incloses, interessats afectats i finalitats, les categories de dades personals, el tipus de tractaments i les seves finalitats així com els destinataris de les dades.

Les mesures dirigides a garantir la seguretat de les dades.

Aplicació dels principis de protecció de dades.

Els drets dels interessats en relació amb el tractament i els mitjans per a exercir-los, així com el dret a presentar reclamació davantl'APD i davant els tribunals.

L'acceptació per part del RT o ET que transfereixen dades de la responsabilitat per qualsevol violació de les BCR per part dels destinataris no establerts a la UE

Els mecanismes interns de supervisió i de cooperació amb l'autoritat de control.

Els procediments de reclamació.

En definitiva, el contingut de les BCR és semblant a un codi de conducta o política de privadesa, de fet el seu contingut comprèn pràcticament tot el programa de privadesa i protecció de dades d'una corporació.

El procediment d'adopció de les BCR es troba en les normes del RGPD dedicades als mecanismes de consistència. L'òrgan competent de l'establiment principal de la corporació a l'EU ha de dirigir-se a l'autoritat principal (competent) i negociar amb ella el contingut de BCR. En emetre una autorització, l'autoritat principal ha de sotmetre-la a l'opinió del Comitè Europeu de Protecció de Dades, que no és directament vinculant.

Un altre instrument per a oferir garanties suficients és l'adhesió a codis de conducta o adhesió a esquemes de certificació, sempre que aquesta adhesió inclogui compromisos vinculants i executables [art. 46.2.e) i f)]. Aquests compromisos vinculants es plasmen quasi sempre a través d'un contracte.

2) Garanties adequades que sí necessiten autorització prèvia. Article 46.3. RGPD:

"Sempre que hi hagi autorització de l'autoritat de control competent, les garanties adequades previstes en l'apartat 1 poden igualment ser aportades, en particular, mitjançant:

a) clàusules contractuals entre el responsable o l'encarregat i el responsable, encarregat o destinatari de les dades personals al tercer país o organització internacional, o (es tracta de les clàusules *ad hoc* autoritzades per APD nacional)

b) disposicions que s'incorporin en acords administratius entre les autoritats o organismes públics que incloguin drets efectius i exigibles per als interessats."

En aquest cas, pot tractar-se per exemple d'un memoràndum d'enteniment entre autoritats públiques de països diferents.

Tots aquests instruments han de contenir drets exigibles i accions legals efectives per als interessats.

Així mateix, les decisions d'APD preses sobre la base de la DPD han de continuaressent vàlides de moment (art. 46.5 RGPD).

3.10.4. Les excepcions per a situacions específiques

Segons preveu l'article 49.1 RGPD, en absència d'una decisió d'adequació o de garanties adequades, una transferència o un conjunt de transferències de dades personals a un tercer país o organització internacional únicament s'ha de dur a terme si es compleix alguna de les condicions següents:

- l'interessat ha donat explícitament el consentiment a la transferència proposada, després d'haver estat informat dels possibles riscos per a ell d'aquestes transferències a causa de l'absència d'una decisió d'adequació i de garanties adequades;

- la transferència és necessària per a l'execució d'un contracte entre l'interessat i el responsable del tractament o per a l'execució de mesures precontractuals adoptades a sol·licitud de l'interessat;

- la transferència és necessària per a la formalització o execució d'un contracte, en interès de l'interessat, entre el responsable del tractament i una altra persona física o jurídica;

- la transferència és necessària per raons importants d'interès públic;

- la transferència és necessària per a la formulació, l'exercici o la defensa de reclamacions;

- la transferència és necessària per a protegir els interessos vitals de l'interessat o d'altres persones, quan l'interessat està físicament o jurídicament incapacitat per a donar el consentiment;

- la transferència es fa des d'un registre públic que, d'acord amb el dret de la Unió o dels estats membres, té per objecte facilitar informació al públic i està obert a la consulta del públic en general o de qualsevol persona que pugui acreditar un interès legítim, però només en la mesura en què es compleixin, en cada cas particular, les condicions que estableix el dret de la Unió o dels estats membres per a la consulta.

Quan una transferència no pot basar-se en disposicions dels articles 45 o 46, incloses les disposicions sobre normes corporatives vinculants, i no és aplicable cap de les excepcions per a situacions específiques a què es refereix el paràgraf primer d'aquest apartat, solament es pot dur a terme si no és repetitiva, afecta solament un nombre limitat d'interessats, és necessària per a les finalitats d'interessos legítims imperiosos perseguits pel responsable del tractament sobre els quals no prevalguin els interessos o drets i llibertats de l'interessat, i el responsable del tractament va avaluar totes les circumstàncies concurrents

en la transferència de dades i, basant-se en aquesta avaluació, va oferir garanties apropiades pel que fa a la protecció de dades personals. El responsable del tractament ha d'informar l'autoritat de control de la transferència. A més de la informació a què fan referència els articles 13 i 14, el responsable del tractament ha d'informar l'interessat de la transferència i dels interessos legítims imperiosos perseguits (així ho estableix l'art. 49.1 *in fine* RGPD).

Quant a les excepcions que planteja el RGPD, tampoc no es plantegen grans novetats. Les excepcions previstes són pràcticament les mateixes que les de la DPD.

Tanmateix, el RGPD introdueix una novetat que consisteix en la possibilitat de transferir dades sobre la base de l'interès legítim del RT.

Això és possible si es compleixen uns determinats paràmetres: limitar-se a supòsits en què les transferències no són repetitives, no se succeeixen en el temps i afecten un nombre limitat d'interessats. Quant a què ha d'entendre's per *nombre limitat d'interessats* és una cosa que s'anirà determinant i analitzant en la pràctica.

El RT en aquest cas ha de dur a terme una ponderació entre el dret a transferir les dades i el dret i interessos dels afectats, i concloure que no prevalen sobre els del RT. En aquest cas, cal establir mesures de salvaguarda. Tot això ha de quedar documentat, i ha d'informar-se l'interessat i l'APD.

Quant al Privacy shield

El Privacy shield es basa en una decisió d'adequació de la Comissió que es va adoptar després del buit que va deixar l'anul·lació dels Principis de port segur (Safe harbour), com a conseqüència de la STJUE en el cas *Schrems*.

Les transferències de dades entre els EUA i Europa, fins a l'anul·lació dels Principis de port segur, es regien per una decisió de la Comissió segons la qual les empreses americanes que complien amb la normativa aprovada es convertien en destinacions segures (*safe harbour*) i se'ls podien transmetre dades.

Després de l'anul·lació dels Principis de port segur, la Comissió i els EUA van negociar un nou marc que permetés l'intercanvi de dades i es va aprovar el Privacy shield. Tanmateix, aquest sistema també està subjecte a força crítiques. El grup de l'article 29 va declarar que aquest acord no complia amb tots els aspectes que exigeix la normativa europea de protecció de dades. El juny de 2017 haurà de procedir-se a una revisió d'aquesta decisió. Així mateix, ha de subratllar-se que Digital Rights Ireland va plantejar una demanda davant el TJUE qüestionant l'acord de Privacy shield i demanant-ne l'anul·lació.

3.11. Responsabilitat i sancions

3.11.1. Responsabilitat administrativa

En plantejar, a l'inici d'aquests materials, les raons de la reforma que va portar a l'adopció del RGPD es va subratllar el fet que hi havia una diversitat legislativa cada vegada més gran entre els estats membres. Potser un dels àmbits en què aquesta diversitat es fa més evident és en relació amb el règim sancionador. Efectivament, hi ha països en què el règim sancionador és pràcticament inexistent, mentre que en altres s'estableixen sancions econòmiques molt importants, que poden arribar fins a 600.000 € de multa (com és el cas d'Espanya).

L'aprovació del RGPD solucionarà aquesta divergència normativa. No obstant això, abans d'examinar quines són les noves claus aportades en el si de la UE, cal analitzar breument el panorama legislatiu espanyol sobre aquest tema.

Una de les característiques de la legislació espanyola de protecció de dades és la distinció entre els fitxers públics i els privats. Aquesta diferenciació també afecta el règim sancionador. Quant als fitxers privats, el règim sancionador es troba principalment en els articles 44 i 45 LOPD, i en el cas dels fitxers relatius a les AP en els articles 46 i 48 LOPD.

Així mateix, quant al règim sancionador, ha de recordar-se que en determinats casos són competents les autoritats de protecció de dades de les CA allà on n'hi hagi i segons les competències que tinguin assumides. Aquest és el cas de l'Autoritat Catalana de Protecció de Dades i de l'Agència Basca de Protecció de Dades.

Quant a l'àmbit subjectiu, els subjectes responsables són els RT i els ET(art. 43.1 LOPD).

Segons disposa l'article 44.1 LOPD, les infraccions es qualifiquen com a lleus, greus o molt greus. Així mateix,aquest precepte enumera les diferents conductes que s'inclouen dins de cada nivell.

En funció de la gravetat, les infraccions estan subjectes a un tipus de sanció (art. 45 LOPD). De tal manera que les infraccions lleus són sancionades amb multa de 900 €a 40.000 €; les greus amb multa de 40.001 €a 300.000 € i les molt greus amb multa de 300.001€ a 600.000 €.

L'article 45.4 LOPD determina els criteris sobre la base dels quals s'ha de graduar la quantia de les sancions. Una mesura important és la que disposa l'article 45.6 LOPD, segons el qual,

"6. Excepcionalment l'òrgan sancionador, ambl'audiència prèvia dels interessats iatesa la naturalesa dels fets i la concurrència significativa dels criterisque estableix l'apartat anterior,pot no acordar l'obertura del procediment sancionador i,en llocseu, advertir el subjecte responsable a fi que, en el termini que l'òrgansancionador determini, acrediti l'adopció de les mesures correctores que siguin pertinents en cada cas, sempre queconcorrin determinats pressupòsits."

Quant a les infraccions comeses per les administracions públiques, la característica principal és que no s'estableixen sancions de tipus econòmic. En els casos en què les infraccions es cometin en fitxers de titularitat pública, l'òrgan sancionador ha de dictar una resolució en què estableixi les mesures que escau adoptar perquè cessin o es corregeixin els efectes de la infracció. Aquesta resolució s'ha de notificar al responsable del fitxer, a l'òrgan del qual depengui jeràrquicament i als afectats si n'hi ha (art. 46. 1 LOPD).

L'òrgan sancionador també pot proposar la iniciació d'actuacions disciplinàries, si són procedents. El procediment i les sancions a aplicar sónels que estableix la legislació sobre règim disciplinari de les administracions públiques(art. 46.2 LOPD).

Finalment, cal tenir en compte els terminis de prescripció. Segons disposa l'article 47.1 LOPD, les infraccions molt greus prescriuen al cap de tres anys, les greus al cap de dos anys i les lleus al cap d'un any. El termini de prescripció comença a comptar-se des del dia en què s'hagi comèsla infracció.

Quant al RGPD, l'article 83 porta per rúbrica: "Condicions generals per a la imposició de multes administratives".

Val la pena subratllar el fet que s'estableixi que cada autoritat de control ha de garantir que la imposició de les multes administratives sigui en cada cas individual efectiva, proporcionada i dissuasiva (art. 83.1).

Les multes administratives s'imposen en funció de les circumstàncies de cada cas individual, i per decidir la imposició d'una multa administrativa i la seva quantia s'ha de tenir en compte els elements recollits en l'article 83.2. *a* a *k*.

En relació amb les quanties, ha de subratllar-se que s'estableix una quantitat que opera com una quantitat màxima, però la sanciótambé pot fixar-se sobre la base d'un determinat percentatge del volum de negoci total. Aquest últim element ha estat acollit favorablement. Les sancions sobre la base d'una quantitat fixa poden ser molt greus per a una empresa i no ser-ho tant per a una altra. En canvi, el fet de fixar la quantitat en concepte de multa sobre la base d'un percentatge sembla més equitatiu.

La tipificació de les sancions (art. 83.4, 5 i 6) és la següent:

- Multa fins a 10.000.000 € o per a empreses es pot establir fins al 2% de volum de negoci anual a escala mundial (s'opta per la de més quantia)
- Multa fins a 20.000.000 € o fins al 4%.

- Multa fins a 20.000.000 € o fins al 4%, en el supòsit d'incompliment de les resolucions d'APD.

3.11.2. Responsabilitat civil

Cal no confondre el règim sancionador previst en la legislació amb els altres supòsits en què com a conseqüència de l'incompliment del que disposa la norma, els interessats pateixin"un dany o lesió en els seus béns o drets" (art. 19 LOPD).

Efectivament, segons disposa l'article 19 LOPD:

> "1. Els interessats que, com a conseqüència de l'incompliment del que disposa aquesta Llei pel responsable o l'encarregat del tractament, pateixin dany o lesió en els seus béns o drets tenen dret a ser indemnitzats.
>
> 2. Quan es tracti de fitxers de titularitat pública, la responsabilitat s'exigeix d'acord amb la legislació reguladora del règim de responsabilitat de les administracions públiques.
>
> 3. En el cas dels fitxers de titularitat privada, l'acció s'ha d'exercir davant els òrgans de la jurisdicció ordinària."

Grimalt, referint-se a l'article 17.3 LORTAD, la redacció del qual és pràcticament

igual a la de l'article 19.1 LOPD en aquest aspecte, estableix el següent:

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

Lectura recomanada

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

En aquest cas, l'existència de danys origina un deure de rescabalar l'afectat (es tracta d'un supòsit de responsabilitat civil). Aquesta RC sorgeix quan el dany o lesió en els drets o béns de l'afectat és conseqüència de l'incompliment d'aquesta Llei. 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.

Efectivament, constitueix una infracció greu [sobre la base de l'article 44.3.h) LOPD],

> "Mantenir els fitxers, locals, programes o equips que continguin dades de caràcter personal sense les degudes condicions de seguretat que es determininper via reglamentària".

El fet mateix de no adoptar o mantenir les degudes mesures de seguretat ja comportaria una sanció per constituir una infracció greu. Però, a més, si a conseqüència d'aquesta falta de seguretat es produeixen danys econòmics a l'afectat (per exemple, algú entra en els seus comptes i en suplanta la identitat), aquesta conducta origina així mateix el deure de rescabalar els perjudicis econòmics i morals ocasionats (responsabilitat civil).

Noteu a més que el destinatari de la quantitat en què consisteix la sanció econòmica o la indemnització és diferent en un cas i un altre. Quan es produeix una infracció de la normativa de protecció de dades, la sanció (la multa) va a parar a l'AAPP (l'APD). En canvi, 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.

Quant al RGPD, el dret a la indemnització i responsabilitat es troba 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 patits".

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 els danys i perjudicis".

Per acabar, també ha de quedar clar que en la mesura que la responsabilitat civil i la responsabilitat administrativa obeeixen a finalitats diferents, poden concórrer totes dues o pot existir l'una sense l'altra.

Bibliografia

Adrian di Pizzo Chiacchio (2016). "Efectos en la jurisprudencia del Tribunal Supremo de la doctrina sentada en el caso *Google Spain*, la interpretación de la responsabilidad de los gestores de motores de búsqueda en la implementación del derecho al olvido digital". *Revista jurídica de Catalunya* (ISSN 1575-0078, vol. 115, núm. 4, pàg. 939-976).

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

Boulanger, M. H.; Moreau, D.; Léonard, T.; Louveaux, S.; Poullet, Y.; Terwangne, C. de. (1997). "La protection des données à caractère personnel en droit communautaire: première partie". *Journal des Tribunaux - Droit Européen* (núm. 40, pàgs. 121-127).

Boulanger, M. H.; Moreau, D.; Léonard, T.; Louveaux, S.; Poullet, Y.; Terwangne, C. de. (1997). "La protection des données à caractère personnel en droit communautaire: première partie". *Journal des Tribunaux - Droit Européen* (núm. 41, pàgs. 145-155).

Burkert, H. (1999). "Privacy-Data Protection: a German/European Perspective". A: *Second symposium of the German American Academic Council's Project "Global Networks and Local Values"* (pàg. 43-69).Massachusetts: Woods Hole. Disponible a: http://www.coll.mpg.de/text/second-symposium-german-american-academic-council%E2%80%99s-project-global-networks-and-local-values-wo

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

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

Goñi Sein, José Luís (2007). *La videovigilancia empresarial y la protección de datos personales: Estudios de protección de datos*. Madrid: Civitas.

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

Guerrero Picó, María del Carmen (2006). *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*. Navarra: Aranzadi.

Hert P.J.A. de; 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).

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, pàgs. 169-192). ISSN 1133-8768.

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

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

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.

Miralles Miravet, S.; Baches Opi, S. (2001). "La cesión de datos de carácter personal: análisis de la legislación vigente y su aplicación a algunos supuestos prácticos". *La Ley* (vol. XXII, núm. 5306).

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

Peguera, M. (2015, 10 d'agost). "The Shaky Ground of the Right to Be Delisted". *18 Vanderbilt Journal of Entertainment & Technology Law 507* (2016). Available at SSRN: https://ssrn.com/abstract=2641876 o http://dx.doi.org/10.2139/ssrn.2641876

Peguera, M. (2015, 1 de juliol). "In the Aftermath of Google Spain: How the 'Right to Be Forgotten' is Being Shaped in Spain by Courts and the Data Protection Authority". *Internati-*

onal Journal of Law and Information Technology (vol. 23, núm. 4, pàg. 325-347). Available at SSRN: https://ssrn.com/abstract=2669081

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

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

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

De Asís Roig, Agustín E. (2002). "Protección de datos y derecho de las telecomunicaciones". A: Javier Cremades; Miguel Ángel Fernández-Ordóñez; Rafael Illescas. *Régimen jurídico de Internet* (pàg. 201-228). Madrid: La Ley.

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

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

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