Legislació sobre protecció de dades

PID_00277677

Josep Cañabate-Pérez
Albert Castellanos Rodríguez
Miquel Colobran Huguet

Temps mínim de dedicació recomanat: 8 hores

Universitat Oberta de Catalunya

Josep Cañabate-Pérez

Professor Serra Húnter al Departament de Dret Públic i Ciències Historicojurídiques de la UAB i col·laborador en el màster universitari de Ciberseguretat i Privacitat de la UOC. Amb caràcter previ a la incorporació com a professor lector va exercir l'advocacia en el camp de la privacitat i el dret digital durant deu anys, en el mateix moment que era professor de la UAB. Compta amb una llicenciatura en Dret per la UAB, així com estudis de postgrau i un doctorat per la UAB, i va rebre el premi extraordinari de doctorat. Ha estat investigador visitant a la UC Berkeley, a la Universitat de Münster, Fordham Law School (NYC) i a la Universitat d'Edimburg.

Albert Castellanos Rodríguez

Mànager responsable de l'àrea de Privacitat i Ciberseguretat de l'oficina d'EY a Barcelona i col·laborador del màster universitari de Ciberseguretat i Privacitat de la UOC. En els últims anys, ha compaginat el desenvolupament professional i l'activitat acadèmica com a docent col·laborador a la UOC i La Salle Campus Barcelona-URL. Disposa d'una llicenciatura en Dret per la UB i la UPC en Dret digital i ciberseguretat respectivament, un postgrau i actualment està finalitzant els estudis de doctorat a la UAB.

Miquel Colobran Huguet

Doctor en Informàtica per la UAB. Consultor a la UOC en el grau i màster d'Informàtica i Multimèdia. Especialment en assignatures sobre administració de sistemes i seguretat, així com informàtica i legislació. Ha confeccionat diversos materials i llibres sobre administració de sistemes, seguretat, informàtica forense i legislació aplicada a tecnologies de la informació. La seva recerca s'emmarca dins de la seguretat, de la influència de les TIC en la societat i de l'enginyeria del coneixement.

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats per la professora: Mònica Vilasau Solana

Primera edició: setembre 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Autoria: Josep Cañabate-Pérez, Albert Castellanos Rodríguez, Miquel Colobran Huguet
Producció: FUOC

Índex

Introducció

Constitueix l'objectiu principal d'aquest mòdul facilitar els coneixements necessaris perquè un professional conegui les obligacions i, per tant, les responsabilitats derivades dels principis aplicables en matèria de protecció de dades de caràcter personal. Es pretén, per tant, proporcionar els instruments teòrics i legislatius indispensables perquè pugui arribar a identificar les conductes que puguin ser constitutives d'infraccions en matèria de protecció de dades, així com la normativa aplicable a aquesta disciplina i que afecta la totalitat d'organitzacions que gestionen dades de caràcter personal.

Davant el nou escenari legislatiu que es planteja, és molt probable que a un professional li sorgeixin nombrosos interrogants en el desenvolupament de la seva feina. Per exemple:

- Què s'entén per dada de caràcter personal? Si s'escau, la bústia de missatges conté dades personals d'un treballador?

- El servidor emmagatzema dades de caràcter personal i, per tant, he d'implementar unes mesures de seguretat determinades. Quines són?

- Si es produeix un accés no autoritzat o un forat de seguretat de les dades, què he de fer? Ho he de notificar a algú?

- En el supòsit de contractar un proveïdor que ha d'accedir a les meves dades personals per prestar-me un servei, què hauria de tenir en compte?

En aquest mòdul s'intentaran exposar les qüestions essencials que permetin solucionar un gran nombre dels interrogants que se suscitin.

En primer lloc, es farà un recorregut sobre què representa la protecció de dades i la motivació que porta el dret a regular-la. Se seguirà amb els conceptes fonamentals i drets que reconeix la nova legislació, tenint en compte que incorpora noves figures per gestionar les dades i nous organismes. S'acabarà amb una revisió sobre les vulneracions que es poden produir en matèria de protecció de dades personals i les sancions que es poden aplicar.

Objectius

Els materials didàctics d'aquest mòdul proporcionen els continguts i les eines imprescindibles per assolir els següents objectius:

1. Identificar les diferents figures que estableix la legislació aplicable en matèria de protecció de dades.

2. Identificar què es pot considerar categoria especial de dades personals, així com les precaucions que s'han d'adoptar per gestionar-les. Especialment en relació amb el titular (la persona física o afectat).

3. Identificar els organismes vinculats a la protecció i com i en quines circumstàncies s'hi ha d'interactuar.

4. Identificar situacions de vulneració de dades i conèixer com abordar la problemàtica.

5. Conèixer aspectes específics, com ara, entre altres, les transferències internacionals de dades de caràcter personal i els drets i obligacions dels subjectes que intervenen en el tractament de dades.

1. La protecció de dades

És evident que la informació s'aprecia per diversos aspectes rellevants. Per exemple, en l'àmbit organitzacional la importància rau en la utilitat per prendre decisions o per la qualitat de secret industrial, per la qual cosa en molts casos es considera l'actiu més important. En altres casos, la informació és fonamental per a les operacions de cada dia, tot i que no sempre és propietat de les empreses, sobretot si es considera que aquestes dades poden pertànyer als clients o usuaris. A causa de la importància de les dades i dels beneficis que poden generar als cibercriminals que busquen apropiar-se'n, contínuament s'observen forats de seguretat relacionats amb la fuita d'informació, en què s'utilitza un conjunt cada vegada més ampli i complex d'atacs per aconseguir les finalitats malicioses. A més, el gran augment de l'ús d'Internet actualment fa necessària una protecció i una regulació que protegeixi les dades de les persones davant d'usos no desitjats. Per això en els últims anys ha guanyat especial rellevància la protecció de dades personals.

La protecció de dades personals se situa dins el camp d'estudi del dret informàtic. Es tracta de la garantia o la facultat de control de la informació enfront del tractament automatitzat o no, és a dir, no només aquella informació que s'allotja en sistemes computacionals, sinó en qualsevol suport que en permeti la utilització, l'emmagatzematge, l'organització i l'accés. En alguns països la protecció de dades té reconeixement constitucional, com a dret humà (o dret fonamental) i en altres és simplement legal.

La diversitat d'informació que es pot associar a una persona és àmplia. Les dades que es consideren personals s'utilitzen per a moltes activitats quotidianes. Però la informació es pot trobar en diferents formes i, amb l'avenç tecnològic, moltes dades relacionades amb els individus s'emmagatzemen, es processen o es transmeten en format digital.

Això expandeix el ventall d'opcions per als cibercriminals que busquen treure profit amb la informació, ja que ara s'utilitzen els mitjans tecnològics per cometre delictes, i en aquest punt la seguretat de la informació és molt important, sobretot perquè cada forat de seguretat relacionat amb una fuita d'informació comporta diverses conseqüències. Les conseqüències són unes o altres en funció de les dades que es roben, el tipus d'empresa que s'ha vist afectada, així com la indústria o el sector als quals pertany l'organització.

Com que Internet s'ha convertit en una realitat omnipresent tant en la vida personal com col·lectiva, segons el Preàmbul de la Llei orgànica 3/208 «correspon als poders públics impulsar polítiques que facin efectius els drets de la ciutadania a Internet amb la promoció de la igualtat dels ciutadans i dels grups

en què s'integren per fer possible el ple exercici dels drets fonamentals en la realitat digital». A diversos països del nostre entorn ja s'ha aprovat normativa que a més reforça els drets digitals de la ciutadania.

Així doncs, el dret fonamental que la protecció de dades vol garantir i protegir és el tractament de les dades personals i els drets fonamentals de les persones físiques; entre altres, el dret a la intimitat personal i familiar.

La protecció de dades tracta la garantia o la facultat de control de la informació enfront del seu tractament mitjançant mitjans automatitzats i no automatitzats.

1.1. Què són les dades personals i les dades sensibles

Es considera dades personals qualsevol informació relacionada amb una persona física que es pugui utilitzar per identificar-la directament o indirectament. Pot ser qualsevol informació: imatge, veu, informació biomètrica, una adreça IP, un nom, una foto, una adreça de correu electrònic, dades bancàries, publicacions en llocs web de xarxes socials, informació mèdica, nom i cognoms, domicili, DNI, dades de geolocalització, dades de consum elèctric, etc.

Aquestes dades ens identifiquen i ens caracteritzen com a individus i determinen les nostres activitats, tant públiques com privades. Cada dada està directament relacionada amb les persones, per tant cada subjecte és propietari de les seves dades personals i decideix si les comparteix o no.

Entre aquestes dades es troben les que identifiquen la persona, o les que permeten tenir comunicació amb el seu titular. També, dades relacionades amb la feina, sobre característiques físiques com la fisonomia, l'anatomia o els trets de la persona. A més, també s'ha de tenir en compte la informació relacionada amb la formació i activitats professionals, dades relatives als seus béns i informació biomètrica.

Com que les dades personals pertanyen al seu titular i no a les entitats que fan servir les bases de dades, s'han posat en marxa diverses iniciatives a tot el món, que busquen protegir les dades personals que es troben en possessió de particulars o de governs, i que fan que la tasca de protegir la informació sigui una responsabilitat compartida entre els usuaris, les empreses que tenen accés a les dades i els governs que han de legislar, així com crear institucions encarregades de regular i fer complir la legislació aplicable sobre aquesta matèria.[1]

(1)En tot cas, el terme *pertànyer* i el concepte de propietat, relatiu a les dades, és discutit. Hi ha diverses concepcions, si bé no correspon a aquestes pàgines aprofundir-hi. Qui hi estigui interessat pot llegir, entre altres articles, Kang, J.; Buchner, B. (2004) «Privacy in Atlantis». *Harvard Journal of Law and Technology* (núm. 1, vol. 18, pàg. 229-267, *vid*. pàg. 248). Disponible a SSRN: http://ssrn.com/abstract=626942.

Figura 1. Classificació de dades personals

Font: elaboració pròpia.

La UE ha ampliat substancialment la definició de dades personals

La Unió Europea ha ampliat substancialment la definició de dades personals i els identificadors *online*, com les adreces IP que ara es consideren dades personals. Altres dades, com la informació econòmica, cultural o de salut mental, també es consideren informació de caràcter personal. Fins i tot les dades pseudononimitzades es poden considerar dades de caràcter personal, perquè poden portar de manera directa o indirecta a identificar una persona física.

Dades personals: tota informació sobre una persona física identificada o identificable («l'interessat»). Es considera persona física identificable tota persona la identitat de la qual es pugui determinar, 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; la protecció de dades tracta la garantia o la facultat de control de la informació enfront del seu tractament automatitzat.

Article 4.1 considerants 26, 28 a 30, 34 i 35 del Reglament (UE) 2016/679, General de Protecció de Dades (a partir d'ara, RGPD).[2]

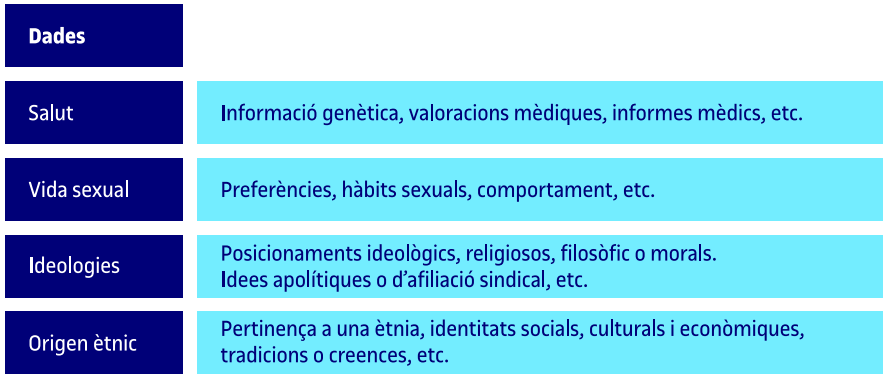
[(2)]Les sigles RGDP es corresponen amb l'acrònim assignat al Reglament europeu de protecció de dades. En els propers apartats ho veureu amb detall.

No totes les dades de caràcter personal són iguals davant la normativa. Hi ha determinades dades que per la rellevància i importància que tenen per a la privacitat s'han de tractar i emmagatzemar amb més cura i complint un seguit de requisits. Aquestes dades s'anomenen *categories especials de dades personals*. Són una categoria de dades que a causa de la incidència especial que tenen en la intimitat, les llibertats públiques i els drets fonamentals de la persona, necessiten més protecció que la resta de dades personals.

Algunes dades personals es poden considerar més sensibles. En aquesta categoria s'inclouen les que involucren l'àmbit privat del titular, l'ús indegut de les quals podria derivar en alguna afectació negativa, com la discriminació, per citar-ne un exemple. Inclouen aspectes com l'origen ètnic o racial, dades

relatives a la salut, conviccions religioses, orientació sexual, afiliació sindical o opinions polítiques. A la figura 2 es pot veure una possible classificació per categories.

Figura 2. Categories especials de dades personals



Font: elaboració pròpia.

Dades sensibles a la LOPD

Amb el RGPD (mitjançant l'article 9), es mantenen les dades que l'antiga LOPD definia com a especialment protegides les dades d'ideologia, religió, creences, origen racial, salut, vida sexual, comissió o infraccions penals o administratives i hi afegeix dues categories més:

- Dades genètiques
- Dades biomètriques

1.2. La normativa de protecció de dades

L'existència de multitud de dades que poden identificar o arribar a identificar una persona, lògicament, provoca que el dret hagi de regular mecanismes per garantir el control de les dades personals, el tractament, mesures per a la protecció i també els drets per actuar en cas de vulneració. Les diferents legislacions comunitàries que tracten la protecció de dades comencen l'any 1995 i el desembre del 2018 s'ha fet l'última adequació (en aquest últim cas en l'àmbit nacional) i, per tant, serà la que veureu en aquests materials.

Només com a informació d'interès, les diferents normatives europees que han existit han estat les següents:

- 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 (derogada).
- 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 (vigent).[3]

[3]Els termes *reglament*, GDPR o RGPD, Reglament (UE) 2016/679 del Parlament europeu o nou reglament de protecció de dades fan referència al mateix, el text del Reglament que es pot consultar a <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES>.

Addicionalment, es troba la legislació espanyola sobre la matèria que, en moltes ocasions, realitza un exercici d'adequació normatiu sobre l'ordenament jurídic espanyol respecte d'allò que estableix la normativa de la UE anteriorment referenciada. Es relaciona a continuació:

- La Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD). Derogada, si bé, s'ha de tenir en compte la disposició derogatòria única de la LOPDGDD.

- 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.

- Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.[4]

[4]Aquesta Llei es coneix, entre altres, per les sigles LOPDGDD.

El RGPD és el marc comú de la Unió Europea pel que fa a la defensa de les dades personals. Abans, cada estat membre disposava de més marge de maniobra per regular segons la seva normativa interna el que n'establia la Directiva 95/46/CE referenciada. Aquest reglament europeu de protecció de dades defineix drets i obligacions comunes a tots els estats membres i a tots els ciutadans europeus, per la qual cosa pretén harmonitzar la disparitat de normatives existents en el context de la Unió Europea.

Sense perjudici que, com el considerant 10 del RGPD estableix:

> «Aquest Reglament també reconeix un marge de maniobra perquè els estats membres especifiquin les seves normes, incloent-hi el tractament de categories especials de dades personals. En aquest sentit, aquest Reglament no exclou que el dret dels estats membres estableixi en quines circumstàncies es preveuen les situacions específiques de tractament i, fins i tot, que estableixi de manera més precisa les condicions en què el tractament de dades personals és lícit.»

La legislació vigent en matèria de protecció de dades es basa en el Reglament (UE) 2016/679, General de Protecció de Dades, que s'articula a Espanya, mitjançant la referenciada Llei orgànica 3/2018, que complementa aquells aspectes en què el RGPD deixa marge de maniobra als estats membres.[5]

[5]En aquests materials es farà menció explícita a la Llei 3/2018 fent-hi referència com a «Llei» i al reglament com a «Reglament», RGPD per intentar articular un discurs coherent i explicatiu.

1.3. Organitzacions subjectes al nou reglament

Segons l'article 3, el Reglament s'aplica al tractament de dades personals, en els següents supòsits:

- en el context de les activitats d'un establiment del responsable o de l'encarregat a la Unió, independentment que el tractament tingui lloc a la Unió o no;

- quan les dades personals dels interessats es trobin a la Unió gestionades per part d'un responsable o un encarregat no establert a la Unió, quan les activitats de tractament estiguin relacionades amb:
  - l'oferta de béns o serveis a aquests interessats a la Unió, independentment de si se'ls requereix el pagament,

  - el control del seu comportament, en la mesura que tingui lloc a la Unió;

- quan un responsable que no estigui establert a la Unió, sinó en un lloc en què el Dret dels estats membres sigui d'aplicació en la virtut del Dret internacional públic.

Si una organització és una pime que tracta dades personals segons el que s'ha descrit més amunt ha de complir el Reglament. Això no obstant, si el tractament de dades personals no constitueix la part principal del negoci i l'activitat no implica riscos per a les persones, no està subjecte a algunes obligacions del RGPD, com per exemple, entre altres, el nomenament d'un delegat de protecció de dades (DPD).[6]

[(6)]És important assenyalar que les «activitats principals» han d'incloure activitats en què el tractament de dades formi una part indissociable de l'activitat del responsable o encarregat del tractament.

Exemple de quan s'aplica el reglament

En el cas d'una empresa petita d'ensenyament superior per Internet i està establerta fora de la UE. La seva activitat va destinada principalment a universitats de llengua espanyola i portuguesa de la UE. Ofereix assessorament gratuït en diversos cursos universitaris i els estudiants necessiten un nom d'usuari i una contrasenya per accedir al material disponible en línia. L'empresa ofereix el nom d'usuari i la contrasenya un cop els estudiants han omplert un formulari de matrícula.

Exemple de quan no s'aplica el reglament

En el cas d'un proveïdor de serveis de fora de la UE que presta serveis a clients de fora de la Unió. Els clients poden utilitzar els serveis quan viatgen a altres països, inclosa la UE. Sempre que no dirigeixi els serveis específicament a persones de la UE no estarà subjecta a les normes del RGPD.

Estan obligades al compliment les organitzacions, empreses, entitats i autònoms que facin ús de les dades personals en l'àmbit comercial dins de la Unió Europea i també fora, sempre que ofereixin serveis a consumidors o usuaris que estiguin dins la UE.

2. Conceptes i definicions

Conceptes i definicions

Algun terme que apareix ara es defineix dins el Reglament. Consulteu el glossari en cas de dubte.

La nova legislació suposa un canvi d'enfocament respecte de la normativa anterior, la Directiva de 1995 i la Llei orgànica 15/1999 de protecció de les dades personals (LOPD), ja que estableix una lògica basada en la responsabilitat proactiva, transparència i l'avaluació i gestió de riscos, mentre que la LOPD es basava en gran part en mecanismes formals com la declaració i l'autorització, que pertanyien a una administració encallada en el passat.

Tota persona té dret a la protecció de les seves dades personals. Basant-se en això, és important saber que no s'haurien de tractar dades de tercers, si no s'han adoptat les mesures necessàries d'informació i transparència i si no existeix una base jurídica que habilita aquest tractament.

2.1. Àmbit d'aplicació del RGPD i exclusions

L'article 2 del RGPD estableix l'àmbit d'aplicació material del Reglament i les exclusions. El RGPD s'aplicarà a tot tractament de dades personals, sigui per mitjans automatitzats o no automatitzats, continguts o destinats a ser inclosos en un fitxer (article 2.1).

El RGPD s'aplica a les persones físiques en relació amb el tractament de les seves dades personals. No és aplicable al tractament de dades relatives a les persones jurídiques, com ara una associació o una fundació.

Sense perjudici de l'anterior, cal destacar segons el que es disposa a la Llei orgànica 3/2018, a l'article 19, que estarà emparat en l'interès legítim el tractament de les dades de contacte i les relatives a la funció o lloc exercit de les persones físiques que prestin serveis a una persona jurídica sempre que es compleixin els següents requisits.

- Que el tractament es refereixi únicament a les dades necessàries per a la localització professional.

- Que la finalitat del tractament sigui únicament mantenir relacions de qualsevol índole amb la persona jurídica a la qual l'afectat presti els serveis.

Igualment, la mateixa presumpció obrarà per al tractament de les dades relatives als empresaris individuals i als professionals liberals, quan únicament s'hi refereixin en aquesta condició i no es tractin per començar-hi una relació com a persones físiques.

No entren en l'àmbit d'aplicació del RGPD els fitxers o conjunts de fitxers que no estiguin estructurats segons els criteris específics. A l'apartat 2n. de l'article 2 del RGPD s'estableixen determinats supòsits en què s'exclou l'aplicació. Aquestes exclusions són les següents:

- Quan es tracti d'una activitat no compresa en l'àmbit del dret de la Unió (UE); es refereix a qüestions relatives a la protecció dels drets i les llibertats fonamentals o a la lliure circulació de dades personals relacionades amb la seguretat nacional.

- Els que realitzin els estats membres (a partir d'ara EM) quan portin a terme activitats relacionades amb la política exterior i de seguretat comuna de la UE.

- Els que realitzin persones físiques en l'exercici d'activitats exclusivament personals o domèstiques. S'entenen per activitats exclusivament personals o domèstiques aquelles que no tinguin cap connexió amb una activitat professional o comercial. El RGPD menciona com a exemples la correspondència i les agendes personals, o l'activitat a les xarxes socials sempre que no s'utilitzin amb finalitats comercials o professionals. Això no obstant, el RGPD sí que s'aplica als responsables o encarregats de tractament que proporcionin els mitjans per tractar dades personals relacionades amb les activitats personals o domèstiques, per exemple, a les xarxes socials com Facebook, Twitter, etc.

- Els que efectuen les autoritats competents amb finalitats de prevenció, recerca, detecció o enjudiciament d'infraccions penals, o d'execució de sancions penals, inclosa la protecció davant d'amenaces a la seguretat pública i a la prevenció.

- Els tractaments de dades personals efectuats per les autoritats competents per a aquests fins es regeixen per la Directiva (UE) 2016/680 del Parlament europeu i del Consell.

- El RGPD tampoc s'aplica a la protecció de dades personals dels difunts. Si bé, deixa en mans dels EM la competència per establir les normes relatives al tractament de les dades personals d'aquestes persones.

2.2. Àmbit d'aplicació territorial

El RGPD s'aplica al tractament de dades personals en el context d'un establiment del responsable o de l'encarregat de tractament (a partir d'ara RT o ET, respectivament) a la Unió Europea, independentment que el tractament tingui lloc dins o fora la UE. Un establiment implica l'exercici de manera efectiva i real d'una activitat per mitjà de modalitats estables, independentment

(7)A l'apartat de subjectes o **figures** veureu amb detall la figura de l'encarregat de tractament i del responsable de tractament.

de la forma jurídica que s'hagi adoptat, sigui una sucursal o una filial amb personalitat jurídica. Addicionalment, cal recordar la definició que s'ha inclòs a l'apartat 1.3.[7]

2.3. Definicions

En moltes ocasions el llenguatge comú no es correspon amb la definició dels termes legals, i en altres necessita ser precisat. Tenint en compte el que s'ha comentat, l'article 4 del RGPD proporciona un seguit de definicions d'alguns dels termes més importants utilitzats al RGPD. També hi ha altres preceptes del RGPD que defineixen alguns termes. Es destaquen els següents.

2.3.1. Dades personals

Tota informació sobre una persona física identificada o identificable («l'interessat»). Es considerarà persona física identificable tota aquella persona de la qual se'n pugui determinar la identitat, directament o indirectament, en particular amb 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.

2.3.2. Categories especials de dades

- **Categories especials de dades (dades sensibles):** dades que revelin l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques, o l'afiliació sindical, les 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 les orientacions sexuals (article 9 de la Llei).

- **Dades genètiques:** dades personals relatives a les característiques genètiques heretades o adquirides d'una persona física que proporcionin una informació única sobre la fisiologia o la salut d'aquesta persona, obtingudes en particular de l'anàlisi d'una mostra biològica d'aquesta persona.

- **Dades biomètriques:** dades personals obtingudes a partir d'un tractament tècnic específic, relatives a les característiques físiques, fisiològiques o conductuals d'una persona física que permetin o confirmin la identificació única d'aquesta persona, com imatges facials o dades dactiloscòpiques.[8]

- **Dades relatives a la salut:** dades relatives a la salut física o mental d'una persona física, inclosa la prestació de serveis d'atenció sanitària, que revelin informació sobre el seu estat de salut. Entre altres: la informació recollida en la inscripció a l'efecte de la prestació d'assistència sanitària, la recollida amb prestació de tal assistència; tot número, símbol o dada assig-

(8)El tractament de fotografies no s'ha de considerar sistemàticament tractament de categories especials de dades personals. Únicament es consideraran dades biomètriques quan el fet que es tractin amb mitjans tècnics específics permeti la identificació o l'autenticació unívoques d'una persona física.

nada a una persona que l'identifiqui de manera unívoca a efectes sanitaris; la informació obtinguda de proves o exàmens, inclosa la procedent de dades genètiques i mostres biològiques; i qualsevol informació relativa a una malaltia, discapacitat, risc de patir malalties; l'historial mèdic, el tractament clínic o l'estat fisiològic o biomèdic de l'interessat, independentment de la font.

2.3.3. Tractament i limitació del tractament

- **Tractament:** qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, sigui per procediments automatitzats o no, com la recollida, registre, organització, estructuració o conservació, adaptació o modificació, extracció, consulta, utilització, comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció.

- **Limitació del tractament:** el dret a la limitació del tractament permet a l'interessat, les dades personals del qual són objecte de tractament, sol·licitar al responsable del tractament que apliqui mesures sobre aquestes dades per, entre altres coses, evitar que es modifiquin, que s'esborrin o se suprimeixin (article 16 de la Llei).

Fitxer enfront de tractament

Al fitxer (que ara s'ha de denominar *tractament*) «clients» se li poden atribuir diferents tractaments, com:

- La prestació d'un servei o venda d'un producte.
- Enviament de publicitat d'altres productes o serveis de l'organització.
- Enviament d'informació sobre esdeveniments organitzats per l'empresa.

Agència Espanyola de Protecció de Dades

L'Agència Espanyola de Protecció de Dades (a partir d'ara, AEPD) assenyala a la guia *Orientaciones y garantías en los procedimientos de anonimización de datos personales* que «l'article 9 del RGPD recomana l'existència d'un equip per a l'estudi de la viabilitat del procés d'anonimització, especialment, si es tracta de dades protegides».

A més, «el personal implicat ha de conèixer i complir tots els aspectes relacionats amb la nova normativa de protecció de dades».

Aquest document es pot consultar al següent enllaç <https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf>.

Addicionalment, la nota tècnica relativa a la K-anonimitat, es pot consultar a <https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-kanonimidad_0.pdf>.

2.3.4. Anonimització o dissociació

És el procés pel qual les dades s'eliminen de manera irreversible. Amb l'anonimització, la dada personal es dissociarà per complet, per la qual cosa un subjecte no podrà ser identificat. Des d'aquest moment, el seu tractament no entraria dins de l'àmbit del Reglament General de Protecció de Dades.

Com a conseqüència, el responsable del tractament podrà fer ús d'aquesta informació ja que no afecta la privacitat de l'individu. Com que és impossible conèixer-ne la identitat, aquesta informació passa a ser una dada empresarial en lloc de personal. No obstant això, l'ús de l'anonimització és molt limitat i cal saber molt bé com realitzar-lo i quan es pot dur a terme.

Finalment, resulta oportú assenyalar que l'AEPD també va tenir ocasió de publicar una nota tècnica relativa a la K-anonimitat, una tècnica utilitzada quan es tracten grans grups de dades i que, entre altres aspectes, permet estudiar el grau d'identificació que podria existir en aquest conjunt de dades suposadament anònim. En conseqüència, permet quantificar fins a quin punt es preserva l'anonimat dels subjectes presents en un conjunt de dades en el qual s'han eliminat els identificadors.

2.3.5. Pseudonimització

El tractament de dades personals de manera que ja no es puguin atribuir a l'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 tractament de dades personals de manera que ja no es puguin atribuir a una persona interessada sense utilitzar informació addicional, sempre que aquesta informació consti per separat i estigui subjecta a mesures tècniques i organitzatives destinades a garantir que les dades personals no s'atribueixen a una persona física identificada o identificable.» (Article 4.5 del RGDP). La pseudonimització només reemplaça una part del conjunt de dades i no permet la identificació directa del subjecte. No obstant això, es pot esbrinar la identitat del subjecte amb informacions addicionals. Per tant, les dades pseudonimitzades estan subjectes al RGPD.[9]

[(9)]Segons el Dictamen 05/14 del Grup de Treball sobre Protecció de Dades de Caràcter Personal de l'article 29, les tècniques de pseudonimització més freqüents són: l'encriptació amb clau secreta, la funció resum, la funció amb clau emmagatzemada, l'encriptació determinista o funció *hash* amb clau d'esborrat de clau i la descomposició en *tokens*.

Exemple de com identificar el subjecte

Es pot canviar el nom, la direcció o la data de naixement d'un subjecte, però no totes les seves dades estaran «emmascarades». Amb informacions complementàries i la realització d'un esforç mínim, es pot arribar a identificar fàcilment aquest subjecte, la qual cosa ens situa dins de l'àmbit de les dades personals i, per tant, del Reglament europeu.

Sense perjudici del que s'ha dit anteriorment, l'Agència Espanyola de Protecció de Dades (AEPD), en col·laboració amb el Supervisor Europeu de Protecció de Dades (EDPS, per les sigles en anglès), va publicar l'informe *Introducción al hash como técnica de seudonimización de datos personales*, un document orientat als responsables de tractaments que utilitzen funcions resum per pseudonimitzar o anonimitzar dades personals. El *hash* és un procés que transforma qualsevol conjunt arbitrari de dades en una nova sèrie de caràcters amb una longitud fixa, amb independència de la mida de les dades d'entrada. El resultat també es denomina *hash* i també resum, *digest* o imatge.

Portant a col·lació les paraules de la mateixa AEPD, cal destacar que les funcions *hash* fa temps que s'utilitzen com a mesura de protecció addicional en el tractament de dades personals. No obstant això, existeixen dubtes de **fins a quin punt el *hash* és una tècnica efectiva de pseudonimització** i si, en determinades circumstàncies, com ara que el missatge original hagi estat eliminat, es pot arribar a considerar que les dades personals estan veritablement anonimitzades.

Introducción al hash como técnica de seudonimización de datos personales

L'AEPD va publicar l'informe *Introducción al hash como técnica de seudonimización de datos personales* el novembre del 2019, que es pot consultar al següent enllaç <https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf>.

La decisió de fer servir tècniques de *hash* adquireix gran importància per determinar, entre altres coses, el compliment efectiu dels drets establerts al RGPD en determinats tipus de tractaments, com poden ser recerca, anàlisi de dades de trànsit o geolocalització, o *blockchain*.

A l'hora de prendre aquesta decisió intervenen consideracions jurídiques, tècniques i de gestió de processos, per la qual cosa els involucrats en la decisió necessiten tenir un coneixement bàsic de les tècniques de *hash* i els seus possibles riscos. Per això, l'estudi introdueix els fonaments de les funcions resum, les propietats, les possibilitats de reidentificar el missatge que va generar el *hash* i recull un conjunt de guies per analitzar l'adequació d'un tractament que utilitzi aquestes funcions.

2.3.6. Fitxer

Fitxer

Per exemple, «fitxers de recursos humans», «fitxer de clients», etc. El RGPD i la LOPDGDD suprimeixen aquesta expressió i la substitueixen per la paraula *tractament*. Ja no es parla de «fitxers de dades personals», sinó de «tractaments de dades personals», encara que aquesta menció es trobi inclosa a l'apartat de definicions del RGPD.

Conjunt estructurat de dades personals accessibles d'acord amb criteris determinats, ja sigui centralitzat, descentralitzat o repartit de forma funcional o geogràfica.

2.3.7. Responsable i encarregat de tractament

Responsable del tractament: persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que, sol o juntament amb d'altres, determina les finalitats i els mitjans del tractament.

Encarregat del tractament: persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que tracta dades personals per compte del responsable del tractament.[10]

(10)En el capítol 7 es veuran amb més detall les figures del responsable i l'encarregat de tractament.

2.3.8. Destinatari

Vegeu també

Per conèixer i aprofundir sobre altres conceptes i definicions, consulteu l'article 4 del RGPD.

Persona física o jurídica, autoritat pública, servei o qualsevol altre organisme al qual es comuniquen les dades, tant si és un tercer com si no. Això no obstant, 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 UE o dels EM.

3. Principis generals

Principis generals

El RGPD ha reformulat els principis de qualitat tradicionals: **proporcionalitat, finalitat, exactitud i actualització, cancel·lació d'ofici i licitud** i es recullen a l'article 5 del RGPD.

3.1. Relatius al tractament de les dades personals

Aquests sis principis que preveu el nou RGPD són, de fet, una versió millorada dels que ja hi havia regulats a la Directiva de 1995 i a la LOPD. I, evidentment, es converteixen en obligacions per al responsable i l'encarregat del tractament. Es podria dir que el principi més significatiu és el de transparència.[11]

(11)El RGPD estableix la transparència com a principi clau, ja que és el camí cap a l'excel·lència en la protecció dels drets dels interessats.

Com més transparents siguin el responsable del tractament i l'encarregat del tractament respecte al titular de les dades (afectat), més bé s'estarà implementant la nova normativa i es podrà disposar de més control sobre l'ús de les seves dades personals. Resulta essencial realitzar un compliment estricte dels deures d'informació i transparència, ja no pel fet de complir amb les normes imposades, sinó per respectar els drets dels afectats i la corresponent esfera d'intimitat.

3.1.1. Principi de minimització de dades

Principi de minimització de dades

Es podria equiparar o podria quedar inclòs a l'antiga LOPD en allò que es coneixia com a principi de proporcionalitat.

Pretén limitar l'ús de dades estrictament a aquelles dades que es considerin adequades, pertinents i limitades en relació amb les finalitats per les quals es van comunicar (article 5.1.c RGPD).

El principi de minimització de dades implica que només es tractaran dades personals quan la finalitat del tractament no es pugui aconseguir raonablement per altres mitjans. En tal cas únicament es tractaran les dades personals adequades i necessàries per aconseguir els fins establerts en el moment de recollir-los (article 5.1.d RGPD).

3.1.2. Principi de limitació de la finalitat

Principi de limitació de la finalitat

Anteriorment es coneixia com a principi de finalitat.

Es reflecteix a l'article 5.1.b. «Les dades personals recollides amb finalitats determinades, explícites i legítimes, i no seran tractades ulteriorment de manera incompatible amb aquestes finalitats; d'acord amb l'article 89, apartat 1, el tractament ulterior de les dades personals amb finalitats d'arxiu en interès públic, finalitats de recerca científica i històrica o finalitats estadístiques no es considerarà incompatible amb les finalitats inicials (article 5.1.b)». No s'està parlant de finalitats diferents, sinó de finalitats incompatibles, ja que en el moment de la recollida no es va informar sobre els tractaments als quals finalment es destinarien les dades.

El principi de limitació de la finalitat del tractament suposa que les dades s'han de recollir per a finalitats determinades, explícites i legítimes i s'han de determinar en el moment de la recollida. També exigeix que no es tractin ulteriorment de manera incompatible amb aquestes finalitats (article 5.1.b RGPD).

Per tant, el tractament de dades personals amb finalitats diferents d'aquelles per les quals s'hagin recollit inicialment no es permet, únicament quan el tractament sigui compatible amb les finalitats per les quals s'hagin recollit inicialment. Conforme al RGPD es consideren finalitats compatibles el tractament ulterior de les dades personals que sigui necessari per al compliment d'una missió en interès públic conferida al RT, empre que es trobin emparats pel Dret de la UE o dels EM.

Per mandat legal no es consideraran incompatibles el tractament ulterior de dades amb les finalitats següents (article 89.1 RGPD):

- Arxiu en interès públic;
- recerca científica i històrica; i
- estadístiques.

En tot cas, per determinar si la finalitat del tractament ulterior és compatible amb la finalitat de la recollida inicial de les dades personals, el RT ha de tenir en compte, segons l'article 6.4 del RGPD, entre altres:

- la relació existent entre les finalitats de la recollida inicial i les finalitats del tractament ulterior;

- el context en què es van recollir les dades, en particular les expectatives raonables de l'interessat pel que fa al seu ús posterior;

- la naturalesa de les dades personals, en particular si es tracta de categories especials de dades personals o dades relatives a condemnes o infraccions penals;

- les possibles conseqüències per als interessats del tractament ulterior previst; i

- l'existència de garanties adequades en l'operació de tractament original i ulterior com, per exemple, l'encriptació i la pseudonimització de les dades.

Si l'interessat va donar el consentiment al tractament o el tractament es basa en el Dret de la UE o dels EM i constitueix una mesura necessària i proporcionada per salvaguardar l'interès públic general, el responsable està facultat per realitzar el tractament ulterior, amb independència de la compatibilitat de les finalitats. Amb tot, haurà de garantir l'aplicació dels principis del RGPD, en particular el relatiu al de transparència per a l'interessat informant-lo sobre aquestes altres finalitats i els drets que l'acompanyen, fins i tot, entre altres, el dret d'oposar-se al tractament.

3.1.3. Principi d'exactitud de les dades

Principi d'exactitud de les dades

Aquest nou principi coincideix en certa manera amb el que es coneixia anteriorment com a principi de la qualitat de les dades.

L'article 5.1.d estableix que 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 respecte a les finalitats per a les quals es tracten» (article 5.1.d RGPD). El nou reglament insisteix en el fet que les dades siguin exactes i actualitzades. Per tant, el responsable del tractament ha d'actuar amb la diligència necessària per fer un bon ús de les dades. És a dir, que siguin correctes, completes i actuals.

Per això el RT ha d'adoptar mesures raonables per suprimir o rectificar sense dilació les dades inexactes que estiguin sota la seva responsabilitat (article 5.1.d RGPD).

3.1.4. Principi de limitació del termini de conservació

Aquest principi té com a objectiu limitar temporalment l'ús de dades personals. Així doncs, obliga a cessar-ne el tractament quan deixen de ser necessàries per a la finalitat que es persegueix. Concretament es troba regulat en els següents termes: «les dades personals es poden conservar durant períodes més llargs, sempre que es tractin exclusivament dades amb finalitats d'arxiu en interès públic». També, «finalitats de recerca científica o històrica o amb finalitats estadístiques, de conformitat amb l'article 89, apartat 1, sense perjudici de l'aplicació de les mesures tècniques i organitzatives adequades que imposa el present Reglament per protegir els drets i les llibertats de l'interessat» (article 5.1.e RGPD).

Si bé el RGPD estableix algunes excepcions a la limitació del termini de conservació sempre que:

- es tractin exclusivament amb finalitats de recerca científica o històrica o finalitats estadístiques, i

- s'apliquin les mesures tècniques i organitzatives adequades per protegir els drets i les llibertats dels interessats.

Per garantir que les dades personals no es conserven més temps del que és necessari, el RT ha d'establir terminis per a la supressió o la revisió periòdica.

3.1.5. Principi d'integritat i confidencialitat

Principi d'integritat i confidencialitat

Anteriorment ja s'aplicaven mesures de seguretat tècnica i organitzativa per protegir les dades personals.

L'objectiu d'aquest principi és garantir una seguretat adequada, la integritat i la confidencialitat de les dades personals. Es troba regulat a l'article 5.1.f en els termes següents: «les dades personals seran 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 adequades» (arti-

cle 5.1.f RGPD). El RGPD pretén protegir els drets dels interessats. Per això, tot i que el principi de seguretat segueix existint, quan s'implementin les mesures concretes s'hauran d'avaluar els riscos que suposa el tractament d'aquestes dades per als drets dels interessats. S'haurà de realitzar una anàlisi de risc que estableixi les mesures de seguretat adequades al risc, aplicar-les i supervisar-les periòdicament, aplicant tècniques d'encriptació de dades, controls d'accés, còpies de seguretat, antivirus, etc. Tot el que sigui necessari per garantir la integritat, la disponibilitat i la confidencialitat de les dades personals.

S'ha de garantir la seguretat de les dades personals i del tractament no autoritzat o il·lícit d'aquestes dades, així com contra la pèrdua, destrucció o dany accidental amb mesures de seguretat tècniques i organitzatives (article 5.2.f RGPD).

A més, per garantir la integritat i la confidencialitat de les dades, el RGPD estableix un seguit d'obligacions que el RT ha de complir. Per exemple, entre altres qüestions, ha de dur a terme una avaluació de riscos preliminar abans de realitzar el tractament de les dades i notificar les violacions de seguretat que puguin succeir a conseqüència del tractament d'aquestes dades.

3.1.6. Principi de licitud, lleialtat i transparència

Principi de licitud, lleialtat i transparència

Amb aquest principi el RGPD pretén deixar enrere els textos carregats de llenguatge jurídic difícil d'entendre dirigits a un consumidor mitjà. Si l'usuari ha de saber què passa amb les seves dades, ha de disposar d'una informació intel·ligible i articulable en un llenguatge clar.

Regulat a l'article 5.1.a, aquest principi pretén exigir que el responsable compleixi amb l'obligació de facilitar a l'interessat la informació relativa al tractament de forma explícita. A més, també concisa, transparent, intel·ligible i de fàcil accés. En concret, l'article diu: «les dades han de ser tractades de manera lícita, lleial i transparent en relació amb l'interessat» (article 5.1.a RGPD).

A més es recorda que, a l'efecte d'allò que s'estableix al RGPD, no són imputables al responsable del tractament (sempre que hagi adoptat totes les mesures raonables perquè se suprimeixin o es rectifiquin sense dilació) la inexactitud de les dades obtingudes directament de l'afectat quan hagi rebut les dades d'un altre responsable en virtut de l'exercici per l'afectat del dret a la portabilitat, o quan el responsable les obtingui del mediador o intermediari quan les normes aplicables al sector d'activitat al qual pertany el responsable del tractament estableixin la possibilitat d'intervenció d'un intermediari o mediador o quan les dades s'hagin obtingut d'un registre públic.

Qualsevol tractament de dades personals ha de ser, a més de lícit, lleial i transparent. Per a la persona ha de quedar totalment clar que s'estan recollint, utilitzant, consultant o tractant les seves dades personals.

El principi de lleialtat i el de transparència van íntimament lligats i exigeixen que s'informi l'interessat de l'existència de l'activitat de tractament i de les finalitats que té. D'acord amb el RGPD el principi de transparència exigeix que tota la informació i comunicació relativa al tractament de les dades personals sigui fàcilment accessible i fàcil d'entendre, i que s'utilitzi un llenguatge senzill

i clar. En particular s'ha de facilitar als interessats la informació sobre la identitat del RT i les finalitats del tractament, i tota la informació necessària de les persones físiques afectades i del seu dret a obtenir confirmació i comunicació de les dades personals que els concerneixin que siguin objecte de tractament.

També s'ha de facilitar la informació complementària que sigui necessària per garantir que el tractament sigui lleial i transparent, atenent les circumstàncies i el context específic del tractament. El RGPD exigeix que s'informi l'interessat de l'existència de l'elaboració de perfils i de les conseqüències que té.

En situacions de complexitat tecnològica o en les quals proliferin diversos agents pot ser convenient que la informació es faciliti de forma electrònica amb un lloc web, especialment quan la informació es dirigeix al públic en general. Podria ser el cas de la publicitat en línia, ja que a l'interessat li resulta difícil saber i comprendre si s'estan recollint les seves dades personals, per qui i amb quina finalitat.

El RGPD preveu una nova modalitat de facilitar informació combinant-la amb icones normalitzades que ofereixin de manera fàcilment visible, intel·ligible i llegible una visió adequada del conjunt del tractament previst. Quan es presentin icones en format electrònic hauran de ser llegibles mecànicament.

En definitiva, les persones físiques han de tenir coneixement dels riscos, les normes, les salvaguardes i els drets relatius al tractament de dades personals, així com de la manera de què disposen per exercir els seus drets en relació amb el tractament de dades que es pugui estar realitzant per part de RT o ET.

La transparència de la informació es configura al RGPD com un dels drets dels interessats, la qual cosa implica que tota la informació que el RT hagi de facilitar a l'interessat ho haurà de fer manera transparent. La informació que el RT hagi de facilitar a l'interessat haurà de ser de forma concisa, transparent, intel·ligible, de fàcil accés, utilitzant un llenguatge clar i senzill, especialment quan la informació es dirigeix a un infant. S'han d'evitar les fórmules enrevessades amb remissions a textos legals. Aquesta informació es pot facilitar per escrit o per altres mitjans. El RGPD preveu la possibilitat que la informació es pugui facilitar verbalment sempre que es demostri la identitat de l'interessat per altres mitjans.

Tal com ja s'ha subratllat, la informació que s'hagi de facilitar als interessats en la recollida de les seves dades personals es podrà realitzar amb una combinació d'icones normalitzades que permetin una visió de conjunt del tractament previst. S'incrementa la informació que el RT ha de facilitar als interessats en el moment de la recollida de les dades personals.

Bibliografia complementària

Per a més informació, es recomana una lectura de la *Guía para el cumplimiento del deber de informar* de l'AEPD que trobareu al següent enllaç <https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes>.

Les Autoritats de Protecció de Dades espanyoles, en el document conjunt que van elaborar, *Guía para el cumplimiento del deber de informar*, aconsellen adoptar un model d'informació per capes, la manera de conciliar els requeriments de proporcionar més informació amb l'exigència de transparència que imposa el RGPD.

3.2. Relatius a la protecció de les dades personals

La Llei orgànica 3/2018, al Títol II, recull els principis generals de protecció de dades de caràcter personal com a exercici de complementarietat d'allò que s'estableix al RGPD en el context espanyol, i els defineix com un conjunt de regles que determinen com recollir, tractar i cedir les dades. En definitiva, són deures als quals estan subjectes els tractaments de dades de caràcter personal.[12]

(12)En el cas que us trobeu llacunes o buits legals, us heu d'inspirar en aquests principis, perquè el tractament de les dades sigui conforme a la normativa.

- **Exactitud (Article 4 Llei).** Les dades han de ser exactes i, si fos necessari, actualitzades. S'han d'adoptar totes les mesures raonables per corregir errors, modificar les dades que resultin ser inexactes o incompletes i garantir la certesa de la informació objecte de tractament.

- **Deure de confidencialitat (Article 5 Llei).** S'ha de garantir una seguretat adequada per preservar la integritat de les dades i impedir-ne l'accés o l'ús no autoritzat. Totes les persones que intervinguin en qualsevol fase del tractament estan subjectes a guardar secret o confidencialitat amb caràcter indefinit.

- **Licitud o legitimació del tractament (Article 6 Llei).**[13] Per tal que el tractament sigui lícit, les dades personals s'han de tractar amb el consentiment explícit de l'interessat o sobre una altra base o fonament jurídic, excloent el que es coneixia com a «coneixement tàcit».
  S'entén per consentiment de l'afectat qualsevol manifestació de voluntat lliure, específica, informada i inequívoca per la qual accepta, sigui amb una declaració o una clara acció afirmativa, el tractament de dades personals que el concerneixen.
  Quan el consentiment de l'afectat en el tractament de les dades sigui per a una pluralitat de finalitats cal que consti de manera específica i inequívoca que aquest consentiment s'atorga per a totes.

(13)En el proper apartat es tracta amb detall aquest article.

- **Licitud o legitimació del tractament de menors d'edat (Article 7 Llei).** Per tal que el tractament sigui lícit, únicament es pot fonamentar en el seu consentiment quan l'interessat del qual es recullen les dades tingui més de catorze anys. En el cas dels menors de catorze anys, només és lícit si consta l'habilitació del titular de la pàtria potestat o tutela, amb l'abast que determinin els titulars de la pàtria potestat o tutela.

- **Tractament de dades per obligació legal, interès públic o exercici de poders públics (Article 8 Llei).** Només es pot considerar fonamentat en

el compliment d'una obligació legal exigible al responsable en els termes previstos a l'article 6.1.c del Reglament (UE) quan així ho prevegi una norma de Dret de la Unió Europea o una norma amb rang de llei, que podrà determinar les condicions generals del tractament i els tipus de dades que en són objecte, així com les comunicacions que procedeixin a conseqüència del compliment de l'obligació legal. Aquesta norma igualment pot posar condicions especials al tractament, com ara l'adopció de mesures addicionals de seguretat o altres d'establertes en el capítol IV del Reglament.

- **Categories especials de dades (Article 9 Llei).** La Llei es remet a l'article 9.2.a del Reglament (UE) 2016/679.

- **Dades de naturalesa penal (Article 10 Llei).**[14] El tractament de dades personals relatives a condemnes i infraccions penals només es pot dur a terme sota la supervisió de les autoritats públiques o quan ho autoritzi el Dret de la Unió o dels estats membres que estableixin garanties adequades per als drets i les llibertats dels interessats. Només es pot portar un registre complet de condemnes penals sota el control de les autoritats públiques.

(14)La Llei es remet a l'article 10 del Reglament.

4. Legitimació del tractament

A partir dels principis que s'han vist, que s'han de complir, ara es passa a veure en quines situacions es pot realitzar el tractament de dades. És a dir, quan és lícit. Per tal que un tractament sigui lícit les dades s'han de tractar amb el consentiment de l'interessat o sobre alguna altra base legítima establerta al RGPD. El RGPD manté el principi recollit a la Directiva 95/46, transferit en el dret espanyol a la LOPD, segons el qual qualsevol tractament de dades s'ha de sustentar en una base jurídica que el legitimi. En aquest sentit el RGPD segueix mantenint les bases jurídiques establertes per la Directiva 95/46. Això no obstant, és important assenyalar la introducció de novetats significatives pel que fa als tractaments sustentats en el consentiment i en l'interès legítim.

Segons l'article 6 de RGPD un tractament lícit ha de complir com a mínim una de les següents condicions:

- L'interessat ha donat el seu consentiment per al tractament de les seves dades personals per a una o diverses finalitats específiques;
- el tractament és necessari per a l'execució d'un contracte en què l'interessat n'és part o per a l'aplicació de mesures precontractuals sol·licitades per l'interessat;
- el tractament és necessari per al compliment d'una obligació legal aplicable al responsable del tractament;
- el tractament és necessari per protegir els interessos vitals de l'interessat o d'una altra persona física;
- el tractament és necessari per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al RT;
- és necessari per a la satisfacció d'interessos legítims perseguits pel RT o per un tercer, sempre que sobre aquests interessos no prevalguin els interessos o els drets i les llibertats fonamentals de l'interessat que requereixin la protecció de dades personals, en particular quan l'interessat sigui un infant.

És important recordar que els principis de licitud o legitimitat en el tractament de dades personals es troben regulats als articles 5 i 6 i en els considerants 41 i 45 a 50 del reglament.

Es desenvoluparan alguns dels aspectes més significatius o que suposen novetats respecte a la legislació anterior.

4.1. Consentiment: atorgament i revocació

El consentiment s'ha de donar mitjançant un acte afirmatiu clar que reflecteixi una manifestació de voluntat lliure, específica, informada i inequívoca de l'interessat d'acceptar el tractament de les dades personals que el concerneixen.

El RT ha de ser capaç de demostrar que l'interessat ha donat el seu consentiment al tractament de les seves dades personals. No es considera que el consentiment s'ha prestat lliurement en els següents supòsits, quan:

- l'interessat no disposa de veritable o lliure elecció;
- l'interessat no pugui denegar o retirar el seu consentiment sense patir cap perjudici;
- hi hagi un desequilibri clar entre interessat i RT, en particular quan el RT sigui una autoritat pública;
- no permeti autoritzar per separat les diverses operacions de tractament tot i ser adequat en el cas concret;
- el compliment d'un contracte, inclosa la prestació d'un servei, sigui dependent del consentiment.

El consentiment inequívoc requereix que es presti mitjançant una manifestació expressa de l'interessat o mitjançant una acció afirmativa clara. A diferència de la legislació anterior, el RGPD no preveu el consentiment tàcit o per omissió.

Hi ha situacions en què el consentiment, a més d'inequívoc, ha de ser explícit:

- quan es tracta de categories especials de dades;
- en els supòsits de transferències internacionals de dades (a partir d'ara, TID);
- quan el tractament de dades projectat suposi l'adopció de decisions individuals automatitzades.

El consentiment es podrà atorgar per escrit, incloent-hi els mitjans electrònics, o mitjançant una declaració verbal. Quan el consentiment es dona amb una declaració escrita que contingui altres assumptes, la sol·licitud de consentiment s'ha de distingir clarament de la resta d'assumptes, ha de ser intel·ligible i s'ha d'utilitzar un llenguatge clar i senzill.

Les formes d'atorgar el consentiment podrien incloure:

- marcar una casella d'un lloc web a Internet, sempre que no estigui premarcada;

- 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 que es tractin les seves dades personals.

Per tant, com s'ha indicat, en cap cas s'entendrà atorgat el consentiment quan apareguin les caselles premarcades, el silenci o la inacció.

El consentiment s'ha de donar per a totes les activitats de tractament realitzades amb la mateixa o les mateixes finalitats. Per tant, quan el tractament tingui diverses finalitats s'ha de donar el consentiment per a totes.

Pel que fa a la revocació del consentiment prestat, l'interessat té dret a retirar el consentiment en qualsevol moment i ha de ser tan fàcil retirar-lo com donar-lo. Els efectes de la revocació sorgiran a partir del moment de la retirada, sense que això afecti la licitud del tractament previ a la retirada.[15]

[15]És un sistema que exigeix una autorització per part de l'interessat abans de l'enviament de qualsevol mena de publicitat per correu electrònic.

Què passa amb els tractaments iniciats abans de l'aplicació del RGPD, la legitimitat dels quals es basa en el consentiment atorgat conforme la Directiva 95/46/CE?

En aquest supòsit no és necessari que l'interessat doni el seu consentiment una altra vegada si la forma en què es va atorgar el consentiment s'ajusta a les condicions del RGPD. Per tant, en aquells casos en què la base del tractament sigui el consentiment tàcit s'ha de sol·licitar el consentiment conforme el RGPD.

Bibliografia complementària

Per saber-ne més podeu consultar *Guidelines on Consent under Regulation* 2016/679 (wp259rev.01) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>.

4.2. Consentiment dels infants

El RGPD considera que s'ha de donar una protecció específica a les dades personals dels menors, ja que els menors solen ser menys conscients dels riscos, les conseqüències i els drets que tenen. En definitiva, es tracta d'un col·lectiu que, per les particularitats especials que té, l'ordenament jurídic el considera vulnerable i, en conseqüència, digne d'una protecció especial.

En el context de l'oferta directa de serveis de la societat de la informació als infants, únicament és vàlid el consentiment del menor que tingui com a mínim setze anys. A més, la informació facilitada al menor s'ha de realitzar en un llenguatge clar i senzill i que li sigui fàcil d'entendre. Si l'infant és menor de setze anys, es requereix l'autorització de qui en tingui la pàtria potestat o la tutela, sense la qual el tractament no és lícit.

Tot i que el RGPD estableix el llindar d'edat a partir del qual el menor pot consentir sense necessitat del titular de la pàtria potestat o tutela, el RGPD deixa oberta la possibilitat perquè els EM estableixin una edat inferior sempre que no sigui inferior a tretze anys. Cal recordar, com s'ha indicat, que l'article 7 de

la Llei orgànica 3/2018 anteriorment referenciada estableix que el tractament de les dades personals d'un menor d'edat únicament es pot fonamentar en el seu consentiment quan tingui més de catorze anys.

El RGPD obliga el RT a realitzar esforços raonables encaminats a verificar que el consentiment va ser donat o autoritzat pel titular de la pàtria potestat o tutela sobre l'infant i l'obliga a realitzar esforços raonables, sobre la base de la tecnologia disponible, així com a tenir-ne prou evidències, segons les obligacions que estableix el RGPD en virtut del principi de responsabilitat proactiva.

4.3. Categories especials de dades

El RGPD atorga una protecció especial a aquelles dades que, per la seva naturalesa, són particularment sensibles en relació amb els drets i les llibertats fonamentals, el tractament de les quals podria suposar riscos importants per als drets fonamentals dels interessats.

Una de les novetats del RGPD respecte a la normativa anterior és la introducció de noves categories especials de dades. Certament, a les que es preveien anteriorment s'afegeixen:

- les dades biomètriques dirigides a identificar de manera unívoca una persona física,
- les dades genètiques.

En principi el RGPD prohibeix el tractament de dades personals que revelin l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques, o l'afiliació sindical, les dades de salut o les relatives a la vida sexual o les orientacions sexuals d'una persona, a més de les dades genètiques i biomètriques (article 9.1 RGPD).

No obstant això, també estableix excepcions a la prohibició general de tractament d'aquesta categoria especial de dades. Són les següents.

- L'interessat ha donat el consentiment explícit per a una o més finalitats especificades.

- En l'àmbit del dret laboral i de la seguretat social, quan el tractament sigui necessari per al compliment d'obligacions i l'exercici de drets específics del RT o del treballador. El tractament es pot realitzar en la mesura en què així sigui autoritzat pel Dret de la UE, dels EM o per un conveni col·lectiu ajustat al dret. A més, s'ha de garantir el respecte als drets fonamentals i als interessos del treballador.[16]

[16] Sobre els tractaments en l'àmbit laboral es pot consultar l'Opinió del GT29 2/2017 *on data processing at work*.

- Quan el tractament sigui necessari per protegir interessos vitals de l'interessat o d'una altra persona física, en el supòsit que l'interessat no estigui capacitat, físicament o jurídicament, per donar el consentiment.

- Quan el tractament es realitzi en el marc d'activitats legítimes per determinades associacions o fundacions, l'objectiu de les quals sigui permetre l'exercici de les llibertats fonamentals i el tractament es refereixi exclusivament als membres actuals o antics. No obstant això, les dades personals no es poden comunicar a tercers sense el consentiment dels interessats.

- Quan el tractament es refereixi a dades personals que l'interessat hagi fet manifestament públics.

- Quan el tractament sigui necessari per raons d'interès públic, en particular en l'àmbit de la salut pública i la gestió dels serveis d'assistència sanitària; amb finalitats de seguretat, supervisió i alerta sanitària per a la prevenció o control de les malalties transmissibles i altres amenaces greus per a la salut; en l'àmbit de la legislació laboral i de protecció social, incloses les pensions.

- De manera excepcional quan el tractament sigui necessari per a l'exercici d'accions judicials o reclamacions en procediments administratius o extrajudicials.

- Amb finalitats d'arxiu en interès públic, de recerca científica i històrica o estadística.

El RGPD també preveu la possibilitat que els EM puguin introduir condicions addicionals, fins i tot limitacions respecte al tractament de les dades genètiques, biomètriques o les dades relatives a la salut.

Bibliografia complementària

Per a més informació sobre l'estudi «Fingerprinting o huella digital del dispositivo» publicat el febrer del 2019 per part de la referida AEPD, es recomana consultar el següent enllaç <https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf>.

Respecte a aquest últim punt, és convenient assenyalar que l'AEPD va publicar l'estudi «Fingerprinting o huella digital del dispositivo», un document que analitza aquesta tècnica d'identificació i rastreig dels usuaris amb els seus dispositius. Per a realitzar-ho, l'Agència va analitzar més de 14.000 llocs web dirigits al públic espanyol, descrivint les tècniques més utilitzades per realitzar aquest perfilat.

Portant a col·lació paraules de la mateixa AEPD, es pot destacar que l'estudi també inclou les mesures que poden posar en marxa els usuaris per mirar d'evitar aquest tipus de seguiment i un seguit de recomanacions a la indústria, tant als fabricants i desenvolupadors com a les companyies que exploten dades obtingudes a partir de l'empremta dels dispositius.

L'empremta digital del dispositiu és un conjunt de dades extretes del dispositiu de l'usuari que permeten individualitzar-lo de manera unívoca. Atès que és habitual que les persones no comparteixin els seus equips, individualitzar

el terminal suposa individualitzar la persona que l'utilitza i, en conseqüència, poder-ne realitzar un perfil. El perfilat no es limita a recopilar i analitzar els hàbits de navegació o les cerques que realitza, sinó a extreure geolocalització, dades de configuració del sistema i de les aplicacions, programes instal·lats, moviments del ratolí, etc. La combinació d'aquesta i d'altra informació que es detalla a l'estudi permet confeccionar una empremta digital única del dispositiu que el singularitza i, per tant, diferencia de manera unívoca cada usuari a Internet.

L'estudi afirma, entre altres conclusions, que de manera molt freqüent aquestes tècniques s'utilitzen per recollir dades de l'equip de l'usuari sense oferir-li informació i sense sol·licitar-li el seu consentiment, i que el conjunt de dades recollides pot ser tan extens o arribar-se a enriquir tant, que pot arribar a recollir fins i tot categories especials de dades.

El document afegeix que, en la majoria dels casos, no es proporcionen eines a l'usuari per poder evitar de manera efectiva la recollida de dades i no se li ofereixen mitjans per exercir els drets establerts al RGPD quan es recullen o s'associen a dades personals.

L'estudi inclou un apartat complet amb recomanacions per a l'usuari, entre les quals es troben utilitzar l'opció *Do not track* del navegador, que permet deixar constància que es vol evitar el seguiment; instal·lar bloquejadors, que permeten evitar la publicitat i el rastreig; deshabilitar l'ús de JavaScript; alternar entre diferents navegadors o executar l'accés a Internet en màquines virtuals. L'estudi de l'AEPD recorda que la navegació privada o d'incògnit no resulta efectiva per prevenir el seguiment i projecta una falsa sensació de seguretat.

4.4. Bases jurídiques diferents del consentiment

El RGPD manté les següents bases jurídiques que legitimen els tractaments de dades personals. Recordeu quines són:

- el consentiment,
- l'existència d'una relació contractual,
- la protecció dels interessos vitals de l'interessat o d'una tercera persona,
- una obligació legal per al RT,
- existència d'un interès públic o l'exercici de poders públics,
- els interessos legítims perseguits pel RT o per tercers als quals es comuniquen les dades.

Una de les novetats que introdueix el RGPD respecte a la legislació anterior és l'obligació del RT d'identificar i documentar la base jurídica que justifica cada tractament. Aquest extrem és indispensable per demostrar que es compleix amb les disposicions del RGPD.

Exemples d'obligacions del RT

- Incloure la base jurídica que justifica el tractament en la informació que es facilita a l'interessat en el moment de la recollida de dades.
- Analitzar abans de realitzar el tractament, i posteriorment a la recollida, especificar i documentar els interessos legítims en què es fonamenten els tractaments en les avaluacions d'impacte o en determinades transferències internacionals de dades.

D'acord amb l'article 6 del RGPD un tractament lícit ha de complir com a mínim una de les següents condicions:

- L'interessat ha donat el seu consentiment per al tractament de les seves dades personals per a una o diverses finalitats específiques.

- El tractament és necessari per a l'execució d'un contracte en què l'interessat n'és part o per a l'aplicació de mesures precontractuals sol·licitades per l'interessat.

- És necessari per al compliment d'una obligació legal aplicable al responsable del tractament.

- Quan el tractament es realitzi en compliment d'una obligació legal aplicable al RT, o quan és necessari per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics, el tractament ha de tenir una base en el Dret de la UE o dels EM. No fa falta que cada tractament individual es regeixi per una norma específica, sinó que n'hi ha prou amb una norma que serveixi de base per a diverses operacions de tractament basades en una obligació legal o per al compliment d'una missió realitzada en interès públic.

- És necessari per protegir els interessos vitals de l'interessat o d'una altra persona física. Les dades personals únicament s'han de tractar sobre la base de l'interès vital de l'interessat quan el tractament no es pugui basar en una altra de les bases jurídiques establertes al RGPD.

- Aquesta mena de tractaments poden respondre tant a motius d'interès públic com als interessos vitals de l'interessat. El RGPD en cita exemples com ara les finalitats humanitàries, incloent-hi el control d'epidèmies o en situacions d'emergència humanitària produïdes per catàstrofes naturals o d'origen humà.

- És necessari per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics que es confereixen al RT. El RGPD menciona com un exemple de missió realitzada en interès públic, sempre que s'ofereixin garanties adequades, l'autorització del tractament de les dades personals sobre les opinions polítiques de les persones.

- És necessari per a la satisfacció d'interessos legítims perseguits pel RT o per un tercer, sempre que no prevalguin els interessos o els drets i les lli-

bertats fonamentals de l'interessat que requereixin la protecció de dades personals, en particular quan l'interessat sigui un infant.

- En aquest supòsit sempre s'ha de realitzar una avaluació i ponderació entre l'interès legítim perseguit pel RT o d'un tercer i els drets i les llibertats dels interessats, tenint en compte les expectatives raonables dels interessats basades en la relació que tenen amb el RT. També s'ha d'avaluar si un interessat pot preveure de manera raonable, en el moment i el context de la recollida de les seves dades personals, que es pugui produir el tractament amb aquesta finalitat.

El RGPD cita alguns exemples d'interès legítim del RT:

- La prevenció del frau quan el tractament de dades personals és estrictament necessari.
- El tractament amb finalitats de màrqueting directe.
- El tractament de dades personals en la mesura estrictament necessària i proporcionada per garantir la seguretat de la xarxa o sistema d'informació. Aquest punt es refereix a la capacitat d'una xarxa o sistema d'informació de resistir, en un nivell determinat de confiança, a esdeveniments accidentals o accions il·lícites o malintencionades que comprometin la disponibilitat, l'autenticitat, la integritat i la confidencialitat de les dades personals conservades o transmeses, i la seguretat dels serveis connexos, o accessibles mitjançant aquests sistemes o xarxes per part d'autoritats públiques, oferts per equips de resposta a emergències informàtiques (CERT), equips de resposta a incidents de seguretat informàtica (CSIRT), proveïdors de xarxes i serveis de comunicacions electròniques i proveïdors de tecnologies i serveis de seguretat. Un exemple seria impedir l'accés no autoritzat a les xarxes de comunicacions electròniques i la distribució malintencionada de codis, frenar atacs de «denegació de servei» i evitar danys als sistemes informàtics i de comunicacions electròniques.
- La transmissió de dades personals dins d'un grup empresarial per a finalitats administratives internes.

En qualsevol cas, la figura de l'interès legítim, tot i que exceptua de la necessitat de sol·licitar un consentiment de l'afectat, sempre s'ha d'utilitzar amb especial cautela, ja que utilitzar-la exigeix un exercici de ponderació respecte als drets i les llibertats dels afectats, sense que els pugui prevaler.

En aquest mateix sentit, el Tribunal de Justícia de la Unió Europea va tenir ocasió de pronunciar-se i va admetre que:

> «Els estats membres disposen que el tractament de dades personals **només es pugui efectuar si [...] és necessari per a la satisfacció de l'interès legítim perseguit pel responsable del tractament o pel tercer o tercers als quals es comuniquen les dades**, sempre que no prevalgui l'interès o els drets i llibertats fonamentals de l'interessat que requereixin protecció segons el que s'estableix a l'apartat 1 de l'article 1 de la present Directiva».

Per tant, d'aquesta manera, amb la finalitat d'efectuar la ponderació necessària exigida, s'ha de plantejar si, ateses les conseqüències concretes que es produeixen en el supòsit de fet que s'està analitzant, l'interès legítim en el tractament de les dades sol·licitades pot prevaler sobre el dret a la protecció de dades dels afectats, les dades dels quals siguin objecte de tractament.

5. Drets de les persones. Regles generals aplicables

La Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades i Garantia dels Drets Digitals (a partir d'ara, «Llei» o «LOPDGDD»), a més de destinar-se a adaptar l'ordenament espanyol al Reglament general de protecció de dades i completar-ne les disposicions, incorpora com a objecte la novetat important de dirigir-se a «garantir els drets digitals de la ciutadania conforme al mandat establert a l'article 18.4 de la Constitució» (article 1.b). Aquest contingut s'ha concretat en el Títol final d'aquesta Llei, el desè, titulat precisament «Garantia dels drets digitals», compost per 19 articles (del 79 al 97).

S'hi reconeix i s'hi regula l'exercici de drets com el de neutralitat de la Xarxa i l'accés universal als drets a la seguretat i l'educació digital, la llibertat d'expressió a Internet, el dret a l'oblit en cercadors i xarxes socials, a la portabilitat, al testament digital, a la intimitat en l'ús dels dispositius digitals en l'àmbit laboral i a la desconnexió digital.

El RGPD preveu un seguit de drets que reconeix la legislació aplicable en matèria de protecció de dades de caràcter personal, coneguts com a drets ARCO en la legislació anterior, afegint-hi dos drets nous: limitació del tractament i portabilitat. A més, estableix la diferència entre el dret de rectificació i el dret de supressió (dret a l'oblit).

5.1. Exercici dels drets

La normativa de protecció de dades permet poder exercir davant el responsable del tractament, o davant l'encarregat del tractament, un seguit de drets, com els drets d'accés, rectificació, oposició, supressió (dret a l'oblit), limitació del tractament, portabilitat i a no ser objecte de decisions individualitzades.

Aquests drets es caracteritzen pel que s'explica tot seguit (article 12 LOPDGDD):

- L'exercici és gratuït.

- Si les sol·licituds són manifestament infundades o excessives (p. ex., caràcter repetitiu) el responsable pot:
  - cobrar un cànon proporcional als costos administratius suportats;
  - negar-se a actuar.

- Les sol·licituds s'han de respondre en el termini d'un mes, tot i que si es té en compte la complexitat i el nombre de sol·licituds, el termini es pot prorrogar dos mesos més.

- El responsable està obligat a informar sobre els mitjans per exercir aquests drets. Els mitjans han de ser accessibles i no es pot denegar aquest dret només pel fet que s'opti per un altre mitjà.

- Si la sol·licitud es presenta per mitjans electrònics, la informació es facilitarà per aquests mitjans quan sigui possible, excepte si l'interessat sol·licita que es faci d'una altra forma.

- Si el responsable no dona curs a la sol·licitud, ha d'informar, com a màxim al cap d'un mes, de les raons de la seva no actuació i la possibilitat de reclamar davant una Autoritat de Control.

- Es poden exercir els drets directament o per mitjà d'un representant legal o voluntari.

- Hi ha la possibilitat que l'encarregat sigui qui atengui la sol·licitud per compte del responsable si tots dos ho han establert en el contracte o acte jurídic que els vincula.

5.1.1. Accés, rectificació, supressió (oblit) i oposició

Dret d'accés (article 13 LOPDGDD)

Els interessats tenen dret a accedir a les dades personals recollides pel RT que els concerneixin, a obtenir del RT confirmació de si s'estan tractant o no les seves dades personals, així com exercir aquest dret amb facilitat dins d'intervals raonables, amb la finalitat de conèixer i verificar la licitud del tractament.

Exemple de dret a dades personals

Els interessats tenen dret a accedir a les dades relatives a les seves històries clíniques que continguin informació sobre diagnòstics, avaluacions de facultatius, resultats de proves o intervencions practicades.

L'interessat té dret a accedir a la següent informació (article 15 RGPD):

- les finalitats del tractament;
- les categories de dades personals tractades;
- els destinataris als quals es comuniquen o es tingui previst comunicar les dades i si es preveu realitzar TID i les garanties que s'aplicaran;
- el termini previst de conservació;
- la possibilitat d'exercir els drets de rectificació, supressió, limitació del tractament o oposició al tractament, i la possibilitat de reclamació davant l'autoritat de control;
- l'existència de decisions automatitzades, inclosa l'elaboració de perfils i, almenys la lògica aplicada i les conseqüències previstes per a l'interessat.

En general, l'accés es farà mitjançant la còpia de les dades personals objecte del tractament i tindrà caràcter gratuït. Si bé, quan l'interessat sol·liciti més d'una còpia, el RT podrà percebre un cànon raonable pels costos administratius. El RGPD també preveu que el RT pugui facilitar l'accés remot a un sistema segur que ofereixi a l'interessat un accés directe a les seves dades personals. A més, quan la sol·licitud d'accés es realitzi per mitjans electrònics la informació es facilitarà per aquests mitjans, tret que l'interessat sol·liciti una altra forma d'accés.

Bibliografia complementària

Per conèixer amb més detall aquests drets, consulteu el següent enllaç de l'AEPD <https://www.aepd.es/reglamento/derechos/index.html>.

El dret d'accés a les dades personals en cap cas afectarà negativament els drets i llibertats de tercers, inclosos els secrets comercials o la propietat intel·lectual, en particular la propietat intel·lectual que protegeix els sistemes informàtics. No obstant això, en cap cas es pot negar a oferir informació a l'interessat.

Quan el RT tingui una gran quantitat d'informació de l'interessat, el RT pot sol·licitar a l'interessat que especifiqui la informació a la qual vol accedir.

El RT ha d'utilitzar les mesures raonables per verificar la identitat dels sol·licitants, en particular quan es prestin serveis en línia.

El RT no pot conservar les dades personals amb l'únic propòsit de poder respondre a les sol·licituds.

Dret de rectificació (article 14 LOPDGDD)

L'exercici d'aquest dret suposa que l'interessat pot obtenir la rectificació de les dades personals pròpies que siguin inexactes sense dilació indeguda del responsable del tractament (article 16 RGPPD). Tenint en compte les finalitats del tractament, es té el dret que es completin les dades personals que siguin incompletes, fins i tot mitjançant una declaració addicional on s'ha d'indicar a quines dades es refereix i la correcció que s'ha de realitzar. A més, quan sigui necessari, s'ha d'acompanyar la sol·licitud de la documentació que justifiqui la inexactitud o el caràcter incomplet de les dades.

Els coneguts drets **ARCO** (accés, rectificació, cancel·lació i oposició) encara coexisteixen. Existien a la LOPD anterior i ara el dret de cancel·lació s'ha ampliat amb el dret de supressió (article 15) o dret a l'oblit i tres drets nous:

- Dret de portabilitat.
- Dret de limitació.
- Dret de decisions automatitzades.

Dret d'oposició (article 18 LOPDGDD)

L'interessat té dret a oposar-se al tractament de les seves dades personals basades en (article 21 RGPD):

- el compliment d'una missió d'interès públic o en l'exercici de poders públics conferits al RT, o;
- en la satisfacció d'un interès legítim del RT;
- fins i tot l'elaboració de perfils sobre la base del que s'ha dit anteriorment.

Aquest dret es pot exercir en qualsevol moment. La conseqüència de l'exercici del dret d'oposició és que el RT deixarà de tractar les dades personals:

- a no ser que acrediti motius legítims imperiosos per al tractament que hauran de prevaler sobre els drets i llibertats de l'interessat, o;
- per a la formulació, l'exercici o la defensa de reclamacions.

Si les dades personals es tracten amb finalitats de màrqueting directe, l'interessat té dret a oposar-se al tractament per a aquestes finalitats, fins i tot a l'elaboració de perfils si està relacionat amb aquest màrqueting directe, independentment que sigui el tractament inicial o ulterior. En aquest supòsit, les dades personals han de deixar de ser tractades per a aquestes finalitats.

Dret de supressió (article 15 LOPDGDD)

El dret que es coneix com a dret «a l'oblit» és el de dret dels interessats al fet que les seves dades personals se suprimeixin i deixin de tractar-se en els supòsits previstos al RGPD (article 17 RGPD). Es pot exercitar aquest dret davant el responsable sol·licitant la supressió de les seves dades de caràcter personal quan es doni alguna de les circumstàncies següents:[17]

(17)Aquest dret de supressió s'amplia de tal forma que el responsable del tractament que hagi fet públiques dades personals adoptarà mesures raonables per indicar als responsables del tractament les que estiguin tractant suprimeixin qualsevol cosa que hi enllaci, o les còpies o rèpliques d'aquestes dades.

- Si les dades personals ja no són necessàries en relació amb les finalitats per les quals van ser recollides o tractades d'una altra forma.

- Si el tractament de les dades personals s'ha basat en el consentiment que es va prestar al responsable i aquest es retira, sempre que el tractament citat no es basi en una altra causa que el legitimi.

- Si l'interessat s'ha oposat al tractament de les dades personals en exercir el dret d'oposició en les circumstàncies següents.[18]
  - El tractament del responsable es fonamentava en l'interès legítim o en el compliment d'una missió d'interès públic, i no han prevalgut altres motius per legitimar el tractament de les teves dades.
  - Que les dades personals siguin objecte de màrqueting directe, incloent-hi l'elaboració de perfils relacionada amb el màrqueting citat.

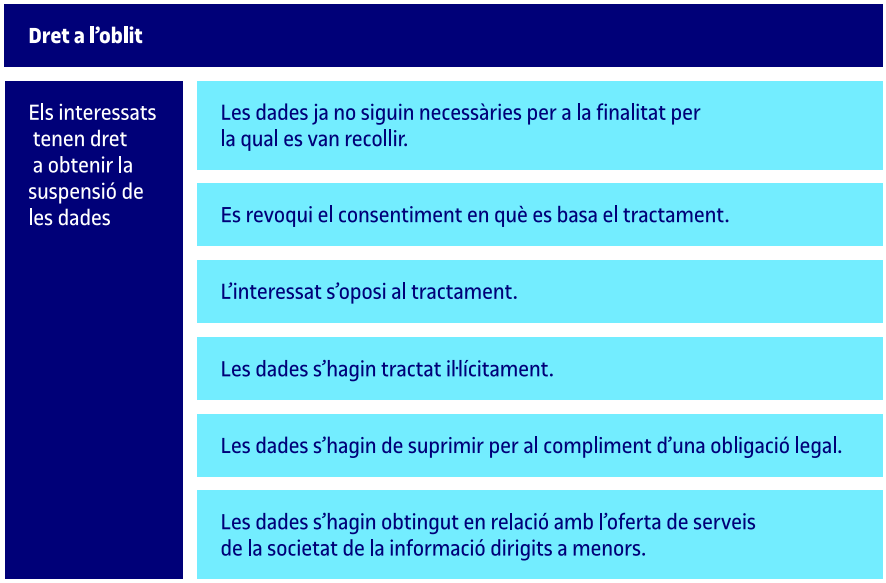
(18)El dret a l'oblit ha estat una de les grans novetats del RGPD.

- Si les dades personals s'han tractat il·lícitament.

- Si les dades personals s'han de suprimir per al compliment d'una obligació legal establerta en el Dret de la Unió o dels estats membres que s'apliqui al responsable del tractament.

- Si les dades personals s'han obtingut en relació amb l'oferta de serveis de la societat de la informació mencionats a l'article 8, apartat 1 (condicions aplicables al tractament de dades dels menors en relació amb els serveis de la societat de la informació).

Figura 3. Dret a l'oblit



Font: elaboració pròpia.

A Internet, quan el RT hagi fet públiques les dades personals, està obligat a indicar als RT que estiguin tractant aquestes dades que suprimeixin qualsevol enllaç que hi porti, o les còpies o les rèpliques de les dades. Per això el RT ha de prendre les mesures raonables, tenint en compte la tecnologia i els mitjans a la seva disposició, per informar de la sol·licitud de l'interessat als responsables que estiguin tractant les dades personals.

El dret de supressió (dret a l'oblit) implica el dret que les dades personals se suprimeixin, així com qualsevol enllaç que contingui informació personal a Internet, o les còpies o rèpliques d'aquestes dades i es deixin de tractar.

Menors

Quan l'interessat va donar el seu consentiment quan era un infant, sense ser plenament conscient dels riscos que implica el tractament, i més tard vol suprimir les dades tractades, també pot exercir aquest dret quan ja és adult.

Això no obstant, aquest dret no és limitat, de manera que pot ser factible no procedir a la supressió quan el tractament sigui necessari per a l'exercici de la llibertat d'expressió i informació, per al compliment d'una obligació legal,

per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable, per raons d'interès públic, en l'àmbit de la salut pública, amb finalitats d'arxiu d'interès públic, en l'àmbit de la salut pública, amb finalitats estadístiques, o per a la formulació, l'exercici o la defensa de reclamacions.

Bibliografia complementària

El redactat s'ha obtingut de la mateixa pàgina web de l'AEPD. Si es vol més informació, es demana que es consulti el següent enllaç <https://www.aepd.es/areas/internet/derecho-al-olvido.html>.

Sense perjudici del que s'ha dit anteriorment, és important recordar que en paraules de la mateixa Agència Espanyola de Protecció de Dades:

> «el dret a l'oblit es pot definir com la manifestació del dret de supressió aplicat als cercadors d'Internet. El dret de supressió ("dret a l'oblit") fa referència al dret a impedir la difusió d'informació personal per Internet quan la seva publicació no compleix els requisits d'adequació i pertinença previstos a la normativa. En concret, inclou el dret a limitar la difusió universal i indiscriminada de dades personals als buscadors generals quan la informació és obsoleta o ja no té rellevància ni interès públic, encara que la publicació original sigui legítima (en el cas dels butlletins oficials o informacions emparades per les llibertats d'expressió o d'informació).»

El Tribunal de Justícia de la Unió Europea (TJUE) va dictar el 13 de maig del 2014 (Assumpte C-131/12) una sentència que estableix, com ja aplicava l'AEPD en les seves resolucions, que el tractament de dades que realitzen els motors de cerca està sotmès a les normes de protecció de dades de la Unió Europea i que les persones tenen dret a sol·licitar, sota certes condicions, que els enllaços a les seves dades personals no figurin en els resultats d'una cerca a Internet realitzada pel seu nom.

5.1.2. Dret a la limitació de tractament (article 16 LOPDGDD)

Article 16 LOPDGDD

Es correspon amb el títol 18 del Reglament.

El dret a la limitació del tractament (article 18 RGPD) suposa que a la solitud de l'interessat el RT ha de limitar l'ús de les dades personals que ha recollit. Generalment consisteix el marcatge de les dades de caràcter personal que es conserven amb la finalitat de limitar-ne el tractament en el futur.

Entre els supòsits per limitar el tractament de dades personals el RGPD preveu les següents: traslladar temporalment les dades seleccionades a un altre sistema de tractament, impedir l'accés d'usuaris a les dades personals seleccionades o retirar temporalment les dades publicades d'un lloc web. En principi, en els fitxers automatitzats la limitació s'ha de realitzar per mitjans tècnics i així fer impossible qualsevol operació de tractament ulterior o modificació de les dades. També s'ha d'indicar clarament en el sistema que el tractament està limitat.

Els supòsits en què es pot sol·licitar la limitació del tractament presenten dues vessants:

- És possible sol·licitar la suspensió del tractament de les dades:
  - quan s'impugni l'exactitud de les dades personals, durant un termini que permeti al responsable fer-ne la verificació;

– quan l'interessat s'hagi oposat al tractament de les dades personals que el responsable realitza basant-se en l'interès legítim o missió d'interès públic, mentre ell verifica si aquests motius prevalen sobre els teus.

- Sol·licitar al responsable la conservació les dades:
  – quan el tractament sigui il·lícit i l'interessat s'ha oposat a la supressió de les seves dades i en lloc seu sol·licita la limitació del seu ús;

  – quan el RT ja no necessiti les dades personals per a les finalitats del tractament, però l'interessat les necessiti per a la formulació, l'exercici o la defensa de reclamacions.

Durant el temps que duri la limitació el RT només pot tractar les dades, més enllà de la conservació, en aquests casos:

- amb el consentiment de l'afectat;
- per a la formulació, l'exercici i la defensa de reclamacions;
- per a la protecció dels drets d'una altra persona física o jurídica;
- per raons d'interès públic.

5.1.3. Dret a la portabilitat (article 17)

La finalitat d'aquest nou dret és reforçar encara més el control de les dades personals, de manera que quan el tractament s'efectuï per mitjans automatitzats, l'interessat pugui rebre les dades personals en un format estructurat, d'ús comú, de lectura mecànica i interoperable, i les pugui transmetre a un altre responsable del tractament, sempre que el tractament es legitimi basant-se en el consentiment o en el marc de l'execució d'un contracte.

No obstant això, aquest dret, per la seva pròpia naturalesa, no es pot aplicar quan el tractament sigui necessari per al compliment d'una missió d'interès públic o en l'exercici de poders públics conferits al responsable.

5.1.4. Dret a no ser objecte de decisions individuals automatitzades (article 22 apartat 1)

Es reconeix el dret a no ser objecte d'una decisió que avaluï aspectes personals relatius a una persona física, basada únicament en el tractament automatitzat i que li produeixi efectes jurídics o l'afecti significativament de manera semblant. Una decisió té efectes jurídics quan els seus drets jurídics es veuen afectats. Per exemple, la denegació automàtica d'una sol·licitud de crèdit en línia o els serveis de contractació en xarxa en què no participa cap intervenció humana.

Informació addicional

Es considera que s'elaboren perfils quan els aspectes personals s'avaluen per elaborar prediccions sobre la persona, fins i tot si no es prenen decisions. Per exemple, si una empresa o organització n'avalua les característiques (l'edat, el sexe, l'alçada) o l'inclou en una categoria, significa que s'està elaborant un perfil sobre un individu.

Les decisions que es basen en algoritmes no poden fer servir categories especials de dades, a no ser que l'afectat hagi donat el seu consentiment o que el procés estigui permès per la legislació de la UE o nacional.

Sobre les decisions individuals automatitzades es poden consultar els articles 21 i 22 i els considerants 71 i 72 del RGPD.

Directrius del Grup de treball de l'article 29 sobre decisions individuals automatitzades i perfilat als efectes del Reglament (UE) 2016/679 (WP 251).

Aquest dret pretén garantir que l'interessat no sigui objecte d'una decisió basada únicament en el tractament de les seves dades, incloent-hi l'elaboració de perfils.

Aquest tractament també es refereix a l'elaboració de perfils que consisteixen en qualsevol forma de tractament de les dades personals que avaluï aspectes personals relatius a una persona física, especialment quan s'analitzi o predigui aspectes relacionats amb el rendiment a la feina, la situació econòmica, la salut, les preferències o interessos personals, la fiabilitat o el comportament, la situació o els moviments de l'interessat, sempre que li produeixin efectes jurídics o l'afecti de manera significativa.

El RGPD preveu determinats supòsits d'excepció, particularment si:

- la decisió és necessària per a l'elaboració o l'execució d'un contracte entre l'interessat i el RT;
- està autoritzada expressament pel Dret de la UE o dels EM, sempre que s'apliquin garanties adequades per salvaguardar els drets i les llibertats de l'interessat;
- es basi en el consentiment explícit de l'interessat.[19]

Les decisions automatitzades i l'elaboració de perfils sobre la base de les categories especials de dades únicament es poden autoritzar en condicions específiques.

En el primer i en el tercer supòsit el RGPD obliga a establir un seguit de salvaguardes per protegir els drets i les llibertats dels interessats entre les quals esmenta: oferir informació específica a l'interessat, el dret a obtenir intervenció humana, a expressar el seu punt de vista, a rebre una explicació de la decisió que s'ha pres després de l'avaluació i a impugnar la decisió.

En tot cas, amb la finalitat de complir amb els principis de lleialtat i transparència aplicables als tractaments de dades personals, el RT ha d'utilitzar procediments matemàtics o estadístics adequats per a l'elaboració de perfils; aplicar les mesures tècniques i organitzatives necessàries per garantir que es corregeixen els factors que introdueixen inexactituds en les dades personals; reduir al màxim el risc d'error; impedir els efectes discriminatoris en les persones físiques o que donin lloc a mesures que produeixin aquest efecte.

(19)Les decisions automatitzades en cap cas poden afectar els menors d'edat.

Bibliografia complementària

«Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679» (wp251rev.01) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.

5.1.5. Limitacions als drets

El RGPD faculta que es puguin imposar restriccions o limitacions en l'exercici dels drets que s'estableixen. Aquestes limitacions s'han d'establir pel Dret de la UE o dels EM mitjançant una llei que ha de respectar els drets i les llibertats fonamentals, a més ha de ser una mesura necessària i proporcionada. Únicament es poden limitar els drets dels interessats per:

- salvaguardar la seguretat de l'Estat, la defensa i la seguretat pública, que inclou la protecció de la vida humana en catàstrofes naturals o d'origen humà;
- prevenir, investigar, enjudiciar infraccions penals o l'execució de les sancions penals;
- complir objectius importants d'interès públic, en particular interessos econòmics o financers de la UE o dels EM, la sanitat pública o la seguretat social;
- prevenir, investigar, enjudiciar infraccions de normes deontològiques en les professions regulades;
- protecció de l'interessat o dels drets o llibertats d'altres, s'hi inclouen la protecció social, la salut pública i les finalitats humanitàries;
- protecció de la independència judicial;
- l'execució de demandes civils.

Aquestes restriccions s'han d'ajustar a allò que es disposa a la Carta i al Conveni Europeu per a la Protecció dels Drets Humans i de les Llibertats Fonamentals, així com en el seu cas, a les corresponents disposicions que puguin resultar aplicables respecte de la legislació vigent en matèria de protecció de dades de caràcter personal.

5.2. Drets digitals dels ciutadans a Internet

Aquest apartat inclou els articles 79 a 82, 96 i 97 de la LOPDGDD.

Drets digitals dels ciutadans a Internet

Concepte aparentment molt més ampli que el de «ciutadans» al qual es refereix l'article 18 de la CE.

- **Dret a la neutralitat d'Internet** (article 80 LOPDGDD). Es reconeix als usuaris d'un dret el contingut del qual es concreta en l'obligació dels pro-

veïdors de serveis d'Internet de proporcionar «una oferta transparent de serveis sense discriminació per motius tècnics o econòmics».

L'article 96 no regula una nova forma testamentària

A diferència del que en pot suggerir el títol, l'article 96 no regula una nova forma testamentària, diferent de les que ja hi ha previstes al Codi civil. Més aviat preveu un contingut específic de les disposicions testamentàries que pot realitzar una persona, referides a una mena concreta de «béns» com poden ser el contingut de la informació «gestionats per prestadors de serveis de la societat de la informació».

- **Dret a l'accés universal a Internet** (article 81 LOPDGDD). S'estableix, en síntesi, que tots tenen dret a accedir a Internet, que «es garantirà» que l'accés sigui «universal, assequible, de qualitat i no discriminatori per a tota la població», incloses les persones que compten «amb necessitats especials». I que «procurarà la superació» de les bretxes de gènere i generacional i atendrà a la realitat específica dels entorns rurals.

- **Dret a la seguretat digital** (article 82 LOPDGDD). Els «usuaris» tenen dret «a la seguretat de les comunicacions que transmetin i rebin per Internet». En aquest cas, s'introdueix una obligació a càrrec dels proveïdors de serveis d'Internet, informar els usuaris dels seus drets (s'entén que, en aquest cas, tot i que no se n'aclareix res més).

- **Dret al testament digital** (article 96 LOPDGDD). L'article 2.2 de la Llei orgànica estableix que no és d'aplicació «als tractaments de dades de persones mortes». Per això, sense perjudici d'allò que es preveu al proper article 3, que fixa els criteris conforme els quals les persones vinculades a la persona morta per raons familiars o, de fet, així com els seus hereus, poden accedir a les dades personals de la persona.

Finalment, l'article 97 de la LOPDGDD (Polítiques d'impuls dels drets digitals) estableix la previsió que el Govern, en col·laboració amb les comunitats autònomes, ha d'elaborar dos documents. D'una banda, el «Pla d'Accés a Internet» orientat a superar les bretxes digitals i garantir l'accés a Internet de col·lectius vulnerables o amb necessitats especials i d'entorns familiars i socials econòmicament desfavorits.

I, d'altra banda, el «Pla d'Actuació» dirigit a promoure les accions de formació, difusió i conscienciació necessàries per aconseguir que els menors d'edat facin un ús equilibrat i responsable dels dispositius digitals i de les xarxes socials i dels serveis de la societat de la informació equivalents d'Internet amb la finalitat de garantir el desenvolupament adequat de la personalitat d'aquests menors i de preservar-ne la dignitat i els drets fonamentals.

5.3. Drets relacionats amb els menors

Aquest apartat inclou els articles 83, 84, 92 i 97.2 (en part) de la LOPDGDD.

- **Dret a l'educació digital** (article 83 LOPDGDD). Orientat a garantir que el sistema educatiu asseguri «la plena inserció de l'alumnat en la societat digital» i l'aprenentatge d'un ús segur i respectuós amb «la dignitat huma-

na, els valors constitucionals, els drets fonamentals i, particularment amb el respecte i la garantia de la intimitat personal i familiar i la protecció de dades personals» dels mitjans digitals.

Per això s'introdueix un mandat directe a totes les «Administracions educatives» per tal que:

– Incloguin en el bloc d'assignatures de lliure configuració la competència digital, així com els elements relacionats amb les situacions de risc derivades de la utilització inadequada de les TIC, amb una atenció especial a les situacions de violència a la xarxa.

– Formar adequadament el professorat en competències digitals i per a l'ensenyament i la transmissió de valors i drets que es refereixen a l'apartat anterior.

– Aquesta inclusió també afecta l'ensenyament universitari, «especialment, aquells que habilitin per al desenvolupament professional en la formació de l'alumnat», que han de garantir «la formació en l'ús i la seguretat dels mitjans digitals i en la garantia dels drets fonamentals a Internet».

– Les Administracions públiques han d'incorporar als temaris de les proves d'accés als cossos superiors i a aquells en què habitualment es desenvolupin funcions que impliquin l'accés a dades personals matèries relacionades amb la garantia dels drets digitals i en particular el de protecció de dades.

- **Protecció dels menors a Internet** (article 84 LOPDGDD). Hi és per reconèixer dues obligacions.[20] Per una banda, estableix que els pares (i mares), tutors, curadors o representants legals dels menors han de procurar («procuraran») que els menors facin un ús «equilibrat i responsable» dels dispositius digitals i dels serveis de la societat de la informació, per garantir el desenvolupament adequat de la personalitat dels menors i preservar-ne la dignitat i els drets fonamentals. D'altra banda, el Ministeri Fiscal ha d'instar («instarà») les mesures cautelars i de protecció previstes a la Llei orgànica 1/1996, de 15 de gener, de Protecció Jurídica del Menor, quan la utilització o la difusió d'imatges o informació personal de menors a les xarxes socials i serveis de la societat de la informació equivalents «puguin implicar» una intromissió il·legítima en els seus drets fonamentals.

- **Protecció de dades dels menors a Internet** (article 92 LOPDGDD). Va dirigit «als centres educatius i qualssevol persones físiques o jurídiques que desenvolupin activitats en què participen menors d'edat» i els imposa l'obligació de garantir «la protecció de l'interès superior del menor i els seus drets fonamentals, especialment el dret a la protecció de dades personals», en la publicació o la difusió de les seves dades personals per mitjà de serveis de la societat de la informació.

(20)Ho fa amb un conjunt d'expressions molt imprecises, que sense cap mena de dubte requeriran la interpretació dels òrgans judicials per concretar-ne l'abast.

En els casos en què aquesta publicació o difusió tingués lloc per mitjà de serveis de xarxes socials o serveis equivalents «han de comptar amb el consentiment del menor o dels seus representants legals», tal com prescriu l'article 7 de la LOPDGDD.

5.4. Drets relacionats amb l'àmbit laboral

Basant-se en el contingut de l'article 18 de la Constitució espanyola (CE) que reconeix com a dret fonamental individual la intimitat personal i la pròpia imatge, l'Estatut dels Treballadors ja va establir originàriament les seves pròpies normes relatives a aquest dret.

Així, l'article 18 en permetre que l'empresa pugui realitzar registres sobre la persona del treballador i els seus efectes, estableix que «en la seva realització es respectarà al màxim la dignitat i intimitat del treballador». L'article 20, en el número 3, indica que «l'empresari podrà adoptar les mesures

que estimi més oportunes de vigilància i control per verificar el compliment del treballador de les seves obligacions i deures laborals, guardant en la seva adopció i aplicació la consideració deguda a la seva dignitat.

Aquest apartat es refereix als articles 87 a 91 de la LOPDGDD.

Aquests cinc articles estan dedicats específicament a l'àmbit laboral (i, en paral·lel, funcionarial o administratiu laboral), en una relació que s'ha de complementar amb el que es disposa en les disposicions finals 13a. i 14a. de la mateixa norma, que modifiquen respectivament l'Estatut dels Treballadors i l'Estatut Bàsic de l'Empleat Públic.

- **Dret a la intimitat i l'ús de dispositius digitals en l'àmbit laboral** (article 87 LOPDGDD). Es reconeix, en primer lloc, que tant els treballadors com els empleats públics «tindran dret a la protecció de la seva intimitat en l'ús dels dispositius digitals que l'ocupador posi a la seva disposició».
  S'estableix l'obligació dels ocupadors d'«establir criteris d'utilització» d'aquests dispositius digitals, incloent-hi l'especificació dels usos autoritzats i, si s'escau, «la determinació dels períodes a què els dispositius es poden utilitzar per a finalitats privades». També s'han d'especificar les possibilitats d'accés per l'ocupador al contingut d'aquests dispositius digitals. S'ha d'informar els treballadors de tot això.

Estàndards mínims de privacitat

La previsió que aquests criteris d'utilització hauran de respectar uns estàndards mínims de privacitat d'acord «amb els usos socials i els drets reconeguts constitucionalment i legal», un fet que sembla subvertir el sistema de fonts del Dret previstes a l'article 1 del Codi civil.

- **Dret a la desconnexió digital en l'àmbit laboral** (article 88 LOPDGDD). No es defineix el contingut precís, però sí que se'n defineix la finalitat. En virtut seva «els treballadors i els empleats públics tindran dret a la desconnexió digital» per garantir, fora del temps de feina, el respecte al temps

de descans, permisos i vacances, així com de la seva intimitat personal i familiar.

Més concretament, s'afegeix que les modalitats d'exercici d'aquest fet «potenciaran el dret a la conciliació de l'activitat laboral i la vida personal i familiar» i se subjectaran al que s'estableix en la negociació col·lectiva o, si s'escau, a allò que s'ha acordat entre l'empresa i els representants dels treballadors.

- **Dret a la intimitat davant l'ús de dispositius de videovigilància i d'enregistrament del so en el lloc de treball** (article 89 LOPDGDD). S'aborda el tema complex de la videovigilància en el lloc de treball, que permet als ocupadors el tractament de les imatges obtingudes, però només «per a l'exercici de les funcions de control dels treballadors o els empleats públics» previstes en la llei amb els límits inherents, i sense que aquests dispositius puguin ser instal·lats en llocs destinats al descans o esbarjo dels treballadors o els empleats públics «com vestuaris, lavabos, menjadors i similars».

  Només s'admet la utilització de sistemes d'enregistrament del so en el lloc de treball en cas de riscos «rellevants» per a la seguretat de les instal·lacions, béns i persones derivats de l'activitat que es desenvolupi al centre de treball i respectant els principis de proporcionalitat i intervenció mínima.

  Aquest ús requereix la prèvia informació, «expressa, clara i concisa», als treballadors i, si s'escau, als seus representants.

- **Dret a la intimitat davant la utilització de sistemes de geolocalització en l'àmbit laboral** (article 90 LOPDGDD). Els sistemes de geolocalització són uns altres dels desenvolupaments tecnològics que permeten tenir més control de l'activitat dels treballadors, que aquesta Llei regula. La Llei autoritza els ocupadors el tractament de les dades obtingudes «a través de sistemes de geolocalització» només per a l'exercici «de les funcions de control dels treballadors o els empleats públics» previstes en «el seu marc legal i amb els límits inherents» i prèvia informació «expressa, clara i inequívoca» als treballadors o els empleats públics i, si s'escau, als seus representants.

- **Drets digitals en la negociació col·lectiva** (article 91 LOPDGDD). La Llei assumeix en tot cas la condició de norma mínima, davant la qual els convenis col·lectius «podran establir garanties addicionals».

5.5. Drets relacionats amb mitjans de comunicació

Aquest apartat inclou els articles 85 i 86 de la LOPDGDD.

- **Dret a la rectificació a Internet** (article 85 LOPDGDD). Es comença reconeixent amb claredat que «tots tenen dret a la llibertat d'expressió a Inter-

net». Així doncs, «els responsables de xarxes socials i serveis equivalents han d'adoptar protocols adequats per possibilitar l'exercici del dret de rectificació», segons «els requisits i procediments previstos en la Llei orgànica 2/1984, de 26 de març, reguladora del dret de rectificació».
L'atenció a la sol·licitud de rectificació dirigida contra un mitjà de comunicació digital ha d'anar acompanyada de la publicació en un lloc visible dels arxius digitals «d'un avís aclaridor que posi de manifest que la notícia original no reflecteix la situació actual de l'individu».

- **Dret a l'actualització d'informacions en mitjans de comunicació digitals** (article 86 LOPDGDD). Aquest article reconeix el dret de «tota persona» a sol·licitar motivadament dels mitjans de comunicació digitals la inclusió d'un avís d'actualització visible amb les notícies que l'afecten «quan la informació que conté la notícia original no reflecteixi la situació actual a conseqüència de circumstàncies que haurien tingut lloc després de la publicació, causant-li un perjudici» i, en particular, quan les informacions originals es refereixin a actuacions policials o judicials que s'hagin vist afectades en benefici de l'interessat per una decisió judicial posterior.

5.6. Dret a l'oblit a Internet

Aquest apartat inclou l'explicació del dret a l'oblit a Internet, regulat en els articles 93 i 94 de la LOPDGDD.

S'estableix un dret de «tota persona» enfront dels motors de cerca a Internet i a l'article 94 de la LOPDGDD enfront dels «serveis de xarxes socials i serveis de la societat de la informació equivalents». Es tracta d'un dret exercitable davant d'un cercador, i també davant un mitjà de comunicació. En aquest mateix sentit, cal recordar que recentment, el Tribunal Constitucional ha establert que els mitjans de comunicació que permetin buscar en les seves hemeroteques digitals per noms propis poden vulnerar el dret a l'oblit de les persones afectades quan no tinguin rellevància pública.

El Constitucional no obliga els mitjans a suprimir de les seves hemeroteques els noms i cognoms de les persones sobre les quals hagin publicat informacions negatives en el passat i ara vulguin exercir el dret a l'oblit, però sí que impedeixen accedir a aquestes notícies mitjançant el criteri de cerca per nom.

- **Dret a l'oblit a Internet** (article 93 LOPDGDD). Els motors de cerca han d'eliminar de les llistes de resultats «que s'obtinguin després d'una cerca efectuada a partir del seu nom», dels enllaços publicats que continguessin «informació relativa a aquesta persona quan siguin inadequats, inexactes, no pertinents, no actualitzats o excessius o hagin esdevingut com a tal pel transcurs del temps», tot això tenint en compte les finalitats per les

quals es van recollir o tractar, el temps que ha transcorregut i la naturalesa i l'interès públic de la informació.

- **Dret a l'oblit en serveis de xarxes socials i serveis equivalents** (article 94 LOPDGDD). Es reconeix el dret de «tota persona» al fet que se suprimeixin, «amb una simple sol·licitud seva», les dades personals publicades a les xarxes socials, facilitades per ella «o per tercers», en aquest cas «quan siguin inadequades, inexactes, no pertinents, no actualitzades o excessives o hagin esdevingut com a tal pel transcurs del temps» o quan les «circumstàncies personals que si s'escau invoqui l'afectat evidenciïn la prevalença dels seus drets sobre el manteniment dels enllaços».

5.7. Dret a la portabilitat

Dret a la portabilitat a les xarxes socials: article 95 de la LOPDGDD.

- **Dret de portabilitats en serveis de xarxes socials i serveis equivalents** (article 95). Es tracta d'una modalitat específica d'un dret per a un àmbit concret. Es tracta del dret a la portabilitat de les dades que els interessats hagin facilitat a un responsable de tractament. Addicionalment, aquest interès també apareix regulat a l'article 20 del RGPD, i l'exercici del qual, segons el que es disposa a l'article 17 de la LOPDGDD s'ha de realitzar «segons el que s'estableix» a l'article 20.
  En virtut d'aquest article, aquests usuaris «tenen dret a rebre i transmetre els continguts que hagin facilitat als prestadors d'aquests serveis», així com al fet que els prestadors «els transmetin directament a un altre prestador designat per l'usuari, sempre que sigui tècnicament possible».

Bibliografia complementària

Per saber-ne més podeu consultar la guia del GT29 sobre portabilitat, aquí <http://ec.europa.eu/newsroom/document.cfm?doc_id=44099>.

El dret a la portabilitat de les dades (article 20 RGPD) es configura com una forma d'accés a les dades personals que permet als interessats rebre les seves dades personals en format estructurat, d'ús comú, de lectura mecànica i interoperable. A més, l'interessat té dret al fet que les dades personals es transmetin directament d'un RT a un altre RT, sempre que sigui tècnicament possible. No obstant això, el dret de l'interessat al fet que les seves dades es transmetin a un altre RT no obliga al RT a adoptar o mantenir sistemes de tractament tècnicament compatibles.

Aquest dret només serà aplicable als tractaments que s'efectuïn per mitjans automatitzats i únicament en dos supòsits:

- quan l'interessat hagi facilitat les dades personals donant el consentiment o,
- quan el tractament sigui necessari per a l'execució d'un contracte.

No s'aplica en relació amb:

- les dades de terceres persones que un interessat hagi facilitat a un responsable;
- el cas que l'interessat hagi sol·licitat la portabilitat de dades que l'incumbeixen però que hagin estat proporcionades al responsable per tercers;
- el tractament que sigui necessari per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable de tractament.

6. Responsabilitat proactiva

Responsabilitat proactiva

Es refereix al concepte de responsabilitat i transparència (*accountability*).

Una de les principals novetats i un concepte essencial que presenta el Reglament General de Protecció de Dades és el principi de responsabilitat proactiva (*accountability*). En termes pràctics, aquest principi requereix que les organitzacions analitzin quina tipologia de dades personals tracten, amb quines finalitats ho fan i quin tipus d'operacions de tractament duen a terme. A partir d'aquest coneixement han de determinar de manera explícita la forma en què aplicaran les mesures que el RGPD preveu, assegurant-se que aquestes mesures són les adequades per complir amb la finalitat per a la qual van ser inicialment recaptades i que poden demostrar-ho davant els interessats i davant les autoritats de supervisió. Ara correspon a les organitzacions la responsabilitat d'identificar els propis focus de risc i triar mesures adequades per mitigar-los.

En síntesi, aquest principi exigeix una actitud conscient, diligent i proactiva per part de les organitzacions davant de tots els tractaments de dades personals que porten a terme.

Tota organització subjecta al reglament ha d'estar en disposició d'acreditar davant qualsevol requeriment de l'organisme competent que:

- Ha avaluat i, en cas necessari, ha redissenyat adequadament els tractaments personals.
- Les mesures de seguretat implementades són adequades i eficaces.
- S'aplica una política interna en matèria de privacitat amb obligacions clares, accions concretes lligades a cada una, i s'han designat responsables del compliment.
- Exigeix aquest mateix compliment responsable als encarregats de tractaments i la cadena de subcontractació.

L'adopció d'una política de protecció de dades personals per part de l'organització que ha de tractar les dades consisteix en una sèrie de mesures i instruments per garantir una protecció òptima de les dades personals tractades.[21] Les més importants són:

- **Anàlisi dels riscos** que suposen els tractaments de dades i quines mesures de seguretat s'han d'aplicar per gestionar-los adequadament i, en cas que sigui necessari, aplicar contramesures i controls per mitigar-los.

[21] Una diferència substancial amb l'antiga llei és que no s'especifiquen de manera concreta quines mesures de seguretat s'han d'implantar, la qual cosa deixa a decisió de cada entitat com i de quina manera es protegiran les dades.

- **Registre d'activitats de tractament**, que busca analitzar quina informació es gestiona, qui són els interessats, quines aplicacions tindran aquests tractaments, quines cessions hi ha previstes, etc. al final, es tracta d'una eina que permet a les organitzacions disposar d'una imatge clara sobre els tractaments de dades personals que es porten a terme.

- **Protecció des del disseny i per defecte.** Això implica que la posada en marxa d'una activitat professional o empresarial, o d'un nou producte o servei, no es pot dur a terme sense haver establert i analitzat les dades que es gestionaran i l'impacte que pugui tenir sobre els drets i les llibertats dels afectats.

- **Les mesures de seguretat** per implantar, que s'hauran d'analitzar i monitorar de forma constant, així com adequades en funció de l'avaluació preliminar de riscos realitzada amb caràcter previ a l'inici d'un tractament de dades de caràcter personal.[22]

- **Notificacions de bretxes de seguretat**, que s'hauran de comunicar abans de 72 hores a les autoritats de control que corresponguin.

- **Avaluació d'impacte en la protecció de dades (EIPD)**, que s'haurà de realitzar amb caràcter previ a la realització del tractament de dades personals. Resultarà d'aplicació en aquells casos en què el tractament de les dades pugui suposar un risc alt per als drets i les llibertats dels usuaris. A més, les avaluacions d'impacte sobre la protecció de les dades (EIPD) permeten identificar els riscos associats al tractament i l'adopció de mesures per a la intervenció.

- **L'avaluació de pràctiques i la implementació de procediments**, inclou la notificació de les violacions de seguretat de les dades o la gestió de sol·licituds d'exercicis de drets dels interessats.

- **Mantenir una documentació** interna que asseguri la traçabilitat de les mesures aplicades i les decisions adoptades.[23]

- Si s'escau, e**l nomenament de la figura del delegat de protecció de dades.**

Per complir amb el principi de responsabilitat proactiva, les organitzacions adopten la figura del responsable del tractament.[24] Així doncs, el responsable del tractament de dades té l'obligació d'aplicar les mesures tècniques i organitzatives apropiades per poder garantir una protecció òptima i poder demostrar que el tractament de dades personals és conforme amb el reglament. És a dir, no n'hi ha prou amb complir amb la normativa de protecció de dades,

(22) Mitjançant l'execució d'aquestes mesures (no totes són obligatòries per a totes les entitats), es garanteix la capacitat del responsable del tractament de dades de demostrar i proporcionar evidències del compliment de protecció de dades.

(23) A l'apartat de les mesures tècniques i organitzatives es veuen amb detall.

(24) Aquest principi també es recull a l'article 5 apartat 2 del RGPD: «El responsable del tractament serà responsable del compliment d'allò que es disposa a l'apartat 1 i capaç de demostrar-ho ("responsabilitat proactiva")».

també s'ha de poder demostrar que s'està complint amb la normativa. Per això, el responsable del tractament de dades ha d'establir procediments mitjançant els quals:

- Pugui garantir l'aplicació de la normativa de protecció de dades.
- Pugui demostrar davant de tercers l'aplicació efectiva i el compliment de la legislació referida.

Aquest principi es defineix com la necessitat que el responsable del tractament apliqui mesures tècniques i organitzatives apropiades per poder garantir una protecció òptima i estar en condicions d'acreditar que el tractament de dades personals és conforme amb les obligacions que estableix el RGPD (article 24.1).

7. Subjectes

La normativa estableix l'existència de la figura del responsable, l'encarregat i el delegat de tractament de dades com uns perfils que desenvolupen un paper molt rellevant per a la correcta aplicació del RGPD.[25]

(25) En els propers apartats es detallen aquestes figures.

- **Responsable del tractament (RT)** de les dades és aquella persona física o jurídica, de naturalesa pública o privada, o bé òrgan administratiu que decideix sobre la finalitat, el contingut i l'ús del tractament de les dades personals.

- **Encarregat de tractament (ET)** és la persona física o jurídica o l'òrgan administratiu que realitza el tractament de les dades per compte del responsable.

- **Delegat de protecció de dades (DPD)** és qui, entre altres funcions, ha de vetllar pel compliment de la normativa en matèria de protecció de dades personals al si de l'organització.[26]

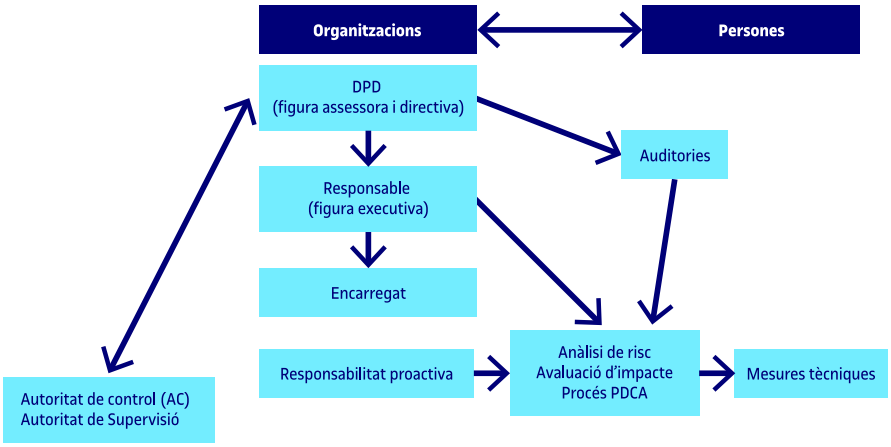
(26) Sovint es fa servir el terme anglosaxó DPO, *Data Protection Officer*, per designar-lo.

Figura 4. Diferència entre les figures

Encarregat del tractament	Responsable del tractament	Delegat de protecció de dades
Persona física o jurídica, de naturalesa pública o privada, o bé l'òrgan administratiu que en l'exercici de la seva activitat tracta amb dades personals. Per llei té l'obligació de determinar com es tracten i es gestionen les dades personals de la seva entitat, fent-se responsable de la creació i la gestió dels fitxers.	Persona física o jurídica, de naturalesa pública o privada, o bé l'òrgan administratiu que en l'exercici de la seva activitat que decideix sobre la finalitat, el contingut i l'ús del tractament de les dades personals.	Ajuda el responsable o l'encarregat del tractament. És un professional amb coneixements especialitzats de la normativa i la pràctica en matèria de protecció de dades. Els DPD poden ser empleats o no del responsable de tractament, però han d'estar en condicions de realitzar les seves funcions de manera independent.

Font: elaboració pròpia.

Figura 5. Esquema de la relació entre tots els elements del reglament



Font: elaboració pròpia.

7.1. Responsable del tractament (RT)

L'article 4.7 del Reglament defineix el responsable del tractament o responsable com «la persona física o jurídica, autoritat pública, servei o un altre organisme que, sol o amb altres, determini 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 podrà establir-los el Dret de la Unió o dels estats membres».[27]

El RT decideix sobre el tractament de les dades personals que ha recollit; així com la finalitat per a la qual s'utilitzaran, els destinataris amb els quals es compartiran, el seu període de conservació, entre altres qüestions del tractament de dades en qüestió.

«El paper primer i primordial del concepte de responsable del tractament és determinar qui ha d'assumir la responsabilitat del compliment de les normes sobre protecció de dades i de quina manera els interessats poden exercir els seus drets en la pràctica. En altres paraules, ha d'assignar la responsabilitat».

[27]Es tracta d'una definició molt àmplia, ja que qualsevol persona física o jurídica, en els termes indicats, que decideixi sobre el tractament de les dades personals es podria considerar responsable del tractament.

En relació amb la definició de *responsable*...

...s'ha de considerar que el Grup de Treball de l'Article 29 (GT29), que es va integrar des del 25 de maig del 2018 al Comitè Europeu de Protecció de Dades (EDPB, segons les sigles en anglès), va publicar un dictamen rellevant sobre aquesta figura. Es tracta del Dictamen 1/2010 sobre els conceptes de «responsable del tractament», WP 169, adoptat el 16 de febrer del 2010. Malgrat que aquest dictamen va ser emès abans del RGPD, moltes qüestions que es regulen en aquest document podrien resultar d'aplicació actualment, sempre que no entrin en col·lisió amb el que s'ha establert per la legislació aplicable en matèria de protecció de dades de caràcter personal.

7.1.1. Funcions, obligacions i responsabilitats

La seva condició de responsable fa que estigui subjecte als requeriments establerts en la normativa i que, en conseqüència, hagi d'observar totes les obligacions que disposi el Reglament General de Protecció de Dades.

Funcions, obligacions i responsabilitats

Algunes d'elles es troben descrites a l'article 32 del Reglament.

El responsable del tractament, com s'ha indicat, decideix sobre l'inici del tractament, les finalitats que té i altres qüestions relatives al tractament de dades personals que eventualment es realitzin. Ha de desenvolupar aquesta finalitat durant tota la «vida» de la dada, és a dir, des que entra a formar part del sistema d'informació fins que s'elimina.

El responsable ha d'informar els afectats de manera transparent quan es produeixi la recollida inicial de les dades personals, i haurà de fonamentar els tractaments de dades personals que realitza sobre alguna de les bases jurídiques exposades amb anterioritat, d'entre les quals destaca, entre altres, el consentiment de l'afectat.

També haurà de determinar si, quan finalitzi la prestació dels serveis de l'encarregat, les dades personals s'han de destruir, s'han de retornar al responsable o lliurar-les, si s'escau, a un nou encarregat. Els treballadors que realitzen el tractament de les dades personals en una organització ho fan en compliment de les funcions que exerceix el responsable del tractament, i també quedaran obligats a un deure de confidencialitat que s'haurà de pactar contractualment entre el responsable i l'encarregat, i s'obligarà aquest últim a traslladar-lo als seus respectius treballadors.

El responsable ha de determinar i aplicar les mesures tècniques i organitzatives adequades per garantir la seguretat de les dades de caràcter personal i evitar-ne l'alteració, la pèrdua, el tractament o l'accés no autoritzat. A més, ha d'estar en condicions de demostrar la conformitat de les activitats de tractament amb el Reglament, inclosa l'eficàcia de les mesures. El fet de no aplicar mesures de seguretat adequades en funció de la tipologia de tractament de dades de caràcter personal que s'estigui duent a terme, podria arribar a suposar una infracció de les obligacions existents i aquesta conducta podria ser sancionable econòmicament.

Algunes de les mesures (article 32) poden ser:

- La pseudonimització i encriptació de dades personals.

- La capacitat de garantir la confidencialitat, la integritat, la disponibilitat i la resiliència permanents dels sistemes i serveis de tractament.

- La capacitat de restaurar la disponibilitat i l'accés a les dades personals de manera ràpida, en cas d'incident físic o tècnic.

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

El responsable, en alguns casos amb l'ajuda de l'encarregat, ha d'establir la probabilitat i la gravetat del risc per als drets i les llibertats de l'interessat amb referència a la naturalesa, l'àmbit, el context i les finalitats que comporta el

tractament que pretén realitzar per als drets i les llibertats per a les persones físiques. El risc s'ha de ponderar mitjançant una avaluació objectiva que determini si les operacions suposen un risc i, si s'escau, si es pot considerar que és alt.

Els riscos de gravetat i probabilitat variables poden provocar danys i perjudicis, en particular en els casos en què:

- puguin donar lloc a problemes de discriminació, usurpació d'identitat o frau, dany en la reputació, pèrdua de confidencialitat o revisió no autoritzada de la pseudonimització; en els casos en què es privi als interessats dels drets o llibertats o se'ls impedeixi exercir el dret sobre les seves dades personals;

- les dades revelin l'origen ètnic o racial, les opinions polítiques, la religió, la militància en sindicats, dades genètiques, etc.;

- s'avaluïn aspectes personals, amb la finalitat de crear o utilitzar perfils personals;

- es tractin dades personals de persones vulnerables, en particular de nens;

- el tractament impliqui una gran quantitat de dades personals i afecti un gran nombre d'interessats.

Amb l'objectiu de demostrar que s'han adoptat les mesures tècniques i organitzatives adequades, el RT ha d'adoptar polítiques internes i aplicar les mesures que consideri oportunes per mitigar els riscos que pugui comportar un eventual tractament de dades de caràcter personal.

La figura del responsable del tractament és fonamental dins del RGPD. Ha de poder demostrar davant de tercers l'aplicació efectiva i el compliment de la normativa de protecció de dades.

Haurà de triar un encarregat del tractament que ofereixi garanties suficients respecte a la implantació i el manteniment de les mesures tècniques i organitzatives, així com verificar que es compleixen les mesures adoptades, preveient si escau, mecanismes d'auditoria mitjançant els contractes.[28]

[28]Els responsables han de triar únicament encarregats que ofereixin garanties suficients per aplicar mesures tècniques i organitzatives adequades, de manera que el tractament sigui conforme amb els requisits del Reglament.
Aquesta previsió s'estén també als encarregats quan subcontracten operacions de tractament amb altres subencarregats.

És a dir...

Sempre que, com a responsables, hàgiu de compartir dades de clients, empleats, subscriptors, etc., amb una altra empresa o un autònom perquè facin una feina a càrrec i risc vostre, que impliqui el tractament d'aquestes dades, s'està parlant d'una relació d'encàrrec

de tractament que implica la presència d'un contracte d'encàrrec que defineixi les condicions del tractament, les finalitats, les obligacions, etc.

7.1.2. Tractament que no requereix identificació

Si les dades personals tractades per un RT no permeten identificar una persona física, el RT no està obligat a obtenir o tractar informació addicional per identificar l'interessat amb l'única finalitat de complir amb el RGPD. En tal cas, el RT ha de ser capaç de demostrar que no pot identificar l'interessat i, quan sigui possible, li ho haurà de comunicar. En aquest supòsit no s'aplicaran les disposicions relatives a l'exercici de drets de l'interessat.

No obstant això, quan amb motiu de l'exercici dels seus drets l'interessat facilita al RT informació addicional, aquest últim no es podrà negar a rebre aquesta informació i, en conseqüència, no es podrà negar a atendre la sol·licitud d'exercici de drets formulada per l'interessat.

La identificació inclou la identificació digital de l'interessat, per exemple, les credencials emprades per l'interessat per obrir una sessió en el servei en línia ofert pel RT.

7.1.3. Corresponsables del tractament

És important recordar que el mateix RGPD defineix el concepte de «tractament» a l'article 4.2 així: «qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, sigui per procediments automatitzats o no, com la recollida, el registre, l'organització, l'estructuració, la conservació, l'adaptació o la modificació, l'extracció, la consulta, la utilització, la comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció».

En el llenguatge del RGPD, caldria remetre's a la figura del «corresponsable del tractament», recollit a l'article 26. Per poder considerar corresponsables del tractament els subjectes intervinents en la relació, cal determinar els elements que marquen aquesta condició:

- L'efectiva participació en la determinació dels objectius i els mitjans de tractament.

- La delimitació de la responsabilitat concreta derivada del RGPD.

En paraules del Tribunal Suprem, a la Sentència 574/2016, de la sala contenciosa administrativa, de 14 de març, parlar de corresponsabilitat suposa un examen de la situació fàctica i comprovar que l'entitat en qüestió té una participació concreta i identificada en la determinació de les finalitats i els mitjans del tractament que es tracti.

El Grup de Treball de l'article 29 (a partir d'ara, GT29), al Dictamen 1/2010, assenyala que: «[...] en el context del control conjunt, la participació de les parts en la determinació conjunta pot revestir diferents formes i el repartiment no ha de ser necessàriament a parts iguals. **De fet, quan hi ha diversos agents, poden tenir una relació molt estreta entre si (i compartir, per exemple, totes les finalitats i els mitjans d'un tractament), o bé una relació més laxa (i, per exemple, compartir-ne només les finalitats o els mitjans, o una part).** Per tant, s'ha de tenir en consideració una àmplia varietat de tipologies de control conjunt i analitzar-se'n les conseqüències legals [...]».

Addicionalment, també apunta el GT29 que: «En alguns casos, diversos agents tracten les mateixes dades personals de manera consecutiva. En tals supòsits, **és probable que, a micronivell, les diferents operacions de tractament de la cadena semblin desconnectades entre si, ja que cada una pot tenir una finalitat diferent. Això no obstant, és necessari fer un doble control per determinar si, a macronivell, aquestes operacions de tractament no s'haurien de considerar un "conjunt d'operacions" que persegueixen una finalitat comuna o utilitzen uns mitjans establerts conjuntament**».

7.2. Encarregat de tractament (ET)

Encarregat de tractament (ET)

Normalment, es tracta d'un tercer que realitza unes determinades tasques per encàrrec del responsable.

L'encarregat de tractament és aquella persona física o jurídica, autoritat pública o servei que, sol o conjuntament amb altres, tracta dades de caràcter personal per compte del responsable de tractament, perquè existeix una relació jurídica que els vincula. És a dir, que el tractament que realitzi un ET s'haurà de regir per un contracte o un altre acte jurídic que vinculi l'encarregat amb el RT i haurà de fixar un contingut mínim. S'hi ha d'establir l'objecte, la durada, la naturalesa i finalitat del tractament, el tipus de dades personals i categories d'interessats, així com les obligacions i drets del responsable, tot això tenint en compte les funcions i responsabilitats específiques de l'encarregat en el context del tractament que es dugui a terme.[29]

[29]La figura de l'ET està regulada a l'article 28 del RGPD i 28 i 33 de la LOPDGDD.

Exemple de què inclou l'ET

L'ET inclou, entre altres, empreses de màrqueting, gestories comptables, empreses de *hosting*, empreses de serveis informàtics, etc.

7.2.1. Funcions, obligacions i responsabilitats

L'acord o acte que se subscriu entre el responsable i l'encarregat del tractament ha de contenir com a mínim les següents obligacions i responsabilitats per a l'encarregat:

- Realitzar el tractament seguint les instruccions documentades del responsable, fins i tot en relació amb les transferències de dades personals a un tercer país o una organització internacional.

- Garantir que les persones autoritzades per tractar dades personals s'hagin compromès a respectar la confidencialitat o estiguin subjectes a una obligació de confidencialitat de naturalesa estatutària.

- Prendre les mesures de seguretat necessàries, segons el que es disposa al RGPD. L'ET haurà d'aplicar les mesures tècniques i organitzatives apropiades per garantir un nivell de seguretat adequat al risc.

- Assegurar que no s'apliquin ni s'utilitzin les dades amb una finalitat diferent de la que figura al contracte.

- Procurar que no es comuniquin les dades, ni per conservar-les, a altres persones.

- Exposar què farà amb les dades un cop finalitzat el servei corresponent.

- Respectar les condicions indicades al RGPD per subcontractar amb un altre encarregat de tractament.

- Assistir el responsable perquè pugui complir l'obligació de respondre les sol·licituds que tinguin per objecte l'exercici dels drets dels interessats. Així mateix, ajudarà el responsable a garantir el compliment de les obligacions previstes al RGPD, és a dir, respecte de la seguretat de les dades l'avaluació d'impacte sobre la protecció de dades.

- Facilitar al responsable la informació necessària per demostrar el compliment de totes les obligacions i d'aquesta manera permetre i contribuir a la realització d'auditories, incloent-hi les inspeccions.

- Informar de manera immediata el responsable en cas que alguna de les instruccions que li siguin traslladades infringeixi el Reglament o altres disposicions en matèria de protecció de dades de la Unió o dels estats membres.

Perquè l'encarregat del tractament pugui accedir a les dades no és necessari el consentiment dels afectats, és a dir, de les persones les dades de les quals es tracten sempre que existeixi el contracte per encàrrec esmentat, atès que, en aquest cas, la base jurídica que legitimaria el tractament d'aquestes dades personals seria l'execució d'un contracte.

Un cop finalitzat el tractament, l'encarregat, a elecció del responsable, ha de retornar o suprimir les dades personals existents, tret que se'n requereixi la conservació en virtut de la normativa vigent (o bé el RT determini que s'han de transmetre les dades a un altre ET).

7.3. Delegat de protecció de dades (DPD)

Delegat de protecció de dades (DPD)

La figura del DPD es regula als articles 37 a 39 del RGPD i als articles 34 a 37 de la LOPDGDD.

La figura del delegat de protecció de dades (DPD o DPO segons les sigles en anglès) és una altra de les novetats del RGPD, tot i que alguns països membres de la UE, com Alemanya, ja comptaven amb aquesta figura abans de l'aprovació del RGPD.

El DPD es configura com la persona amb coneixements especialitzats en dret (no necessàriament un llicenciat en Dret) la normativa i la pràctica en matèria de protecció de dades. A més, en funció de les operacions de tractament que dugui a terme l'organització, el DPD haurà de tenir diferent nivell de coneixements especialitzats.

S'ha de garantir la seva independència dins de l'organització i evitar qualsevol conflicte d'interessos.[30] Quan es tracti d'un DPD extern a l'organització, la relació jurídica entre tots dos s'ha de basar en un contracte de serveis. En determinats supòsits també és possible designar un únic DPD per a diverses organitzacions (article 37.2 i 3 DPD). És obligació del RT publicar les dades de contacte del DPD i, a més, comunicar-les a l'autoritat de control. Per preservar la seva independència no pot rebre cap instrucció del RT (o de l'ET) en el desenvolupament de les seves funcions, ni pot ser destituït o sancionat per motius relacionats en el correcte desenvolupament de les seves tasques laborals.

[30]Per tant, desenvoluparan les funcions de manera independent. Els DPD podran ser empleats o no del RT o ET.

La posició del DPD en l'organització ha de ser al nivell d'altres directors, ja que el RGPD assenyala que ha de retre comptes directament al més alt nivell jeràrquic. En definitiva, ha de ser una persona de comandament intermedi, amb coneixement de l'organització i que ostenti canal directe amb la direcció.

Un altre aspecte que s'ha de tenir en compte és la possibilitat que es produeixi un conflicte d'interessos a conseqüència de l'exercici de funcions com a DPD. El Reglament permet que el DPD pugui exercir altres funcions en l'organització, tot i que únicament ho podrà fer si no es produeix un conflicte d'interessos (article 38.6 RGPD).[31]

[31]Per determinar si hi ha conflicte d'interessos és necessari estudiar cas per cas, ja que la casuística pot ser molt variada.

Exemple de conflicte d'interessos

En determinades situacions queda clar que es produeix aquest conflicte. Seria el cas d'un DPD que exerceixi una altra posició en l'organització en la qual pugui determinar finalitats o mitjans del tractament. Un exemple clar seria un DPD que al mateix temps és responsable de seguretat segons el que estableix l'Esquema Nacional de Seguretat.

El delegat de protecció de dades és la persona que actua com a interlocutor del responsable o encarregat del tractament davant l'Agència Espanyola de Protecció de Dades i les autoritats autonòmiques de protecció de dades que hi pugui haver.

A més, és el responsable de garantir que es compleixi amb la normativa de protecció de dades en el context de l'empresa o organització.

Bibliografia complementària

Es pot consultar aquest registre de DPD al següent enllaç <https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/consultaDPD.jsf>.

Hi ha un registre oficial dels diferents Delegats de Protecció de Dades que han designat les organitzacions. Aquesta consulta es pot efectuar per mitjà de la seu electrònica de l'Agència Espanyola de Protecció de Dades.

Finalment, els responsables i encarregats de tractament comunicaran en el termini de deu dies a l'Agència Espanyola de Protecció de Dades i, si s'escau, a les autoritats autonòmiques de protecció de dades, les designacions, nomenaments i cessaments dels delegats de protecció de dades, tant en els supòsits en què l'empresa estigui obligada com en el cas en què la designació sigui voluntària.

7.3.1. Funcions, obligacions i responsabilitats

Funcions

Les funcions mínimes del DPD es preveuen a l'article 39 RGPD.

Documentació relacionada

Epígraf 4t. del document elaborat pel GT Art.29 *Guidelines on Data Protection Officers* <https://ec.europa.eu/newsroom/document.cfm?doc_id=44100>.

GT Art.29 *Guidelines on Data Protection Officers* <http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf>.

- **Assessorar** el responsable o l'encarregat de tractament.

- **Inspeccionar els procediments** relacionats amb el compliment del RGPD i emetre recomanacions en l'àmbit de les seves competències.

- **Informar i assessorar** els empleats que s'ocupin del tractament sobre les obligacions que els incumbeixen en virtut del RGPD i d'altres disposicions de protecció de dades de la Unió o dels estats membres.

- **Supervisar el compliment del Reglament.** És a dir, de les normes incloses al RGPD, així com d'altres disposicions de protecció de dades de la Unió o dels estats membres i de les polítiques del responsable o de l'encarregat del tractament en matèria de protecció de dades personals.

- **Assessorar pel que fa a l'avaluació d'impacte** relativa a la protecció de dades a què s'enfronta l'organització i supervisar-ne l'aplicació. Això es deu al fet que amb el nou Reglament ja no s'han d'inscriure els fitxers de dades a l'AEPD ni les dades personals estan subjectes, com a l'antiga llei, als nivells de seguretat alta, mitjana o baixa.

- **Supervisar l'aplicació de les normes** per l'encarregat de tractament en matèria de protecció de dades personals. Dins d'aquest apartat s'inclouen: assignació de responsabilitats, formació del personal i auditories corresponents.

- **Actuar com a punt de contacte** de l'organització davant l'Agència Espanyola de Protecció de Dades (AEPD), així com qualssevol altres autoritats de control que hi pugui haver en relació amb el tractament de dades i la realització de consultes.

- **Supervisar la documentació**, notificació i comunicació de les violacions de dades personals.

- **Supervisar la resposta a les sol·licituds de l'autoritat de control** i cooperar-hi per sol·licitud seva o per iniciativa pròpia.

- **Actuar com un punt de contacte** per a qüestions relatives al tractament, tant respecte a l'autoritat de control com als interessats.

El delegat de protecció de dades ha de vetllar perquè es compleixi la normativa de protecció de dades a les organitzacions i ha de tenir una relació estreta amb les autoritats amb competències sobre aquesta matèria.

7.3.2. Obligatorietat de la figura del DPD

Obligatorietat de la figura del DPD

El RGPD exigeix que es nomeni un DPD en els casos que es preveuen a l'article 37.

El DPD no és obligatori per a totes les empreses. L'obligatorietat n'és necessària:

- Quan el tractament el porta a terme una autoritat o organisme públic, excepte els tribunals quan actuïn en l'exercici de la funció judicial.

- En els tractaments a gran escala que per la naturalesa que tenen, l'abast o les finalitats requereixin una observació habitual i sistemàtica d'interessats, com la creació de perfils.

- Les activitats principals del responsable o de l'encarregat consisteixin en el tractament a gran escala de categories especials de dades personals d'acord amb l'article 9 i de dades relatives a condemnes i infraccions penals a les quals es refereix l'article 10.

7.3.3. Organitzacions que han de tenir DPD

Per part seva, la LOPDGDD assenyala, a l'article 34, que els responsables i els encarregats del tractament han de designar, si més no, un delegat de protecció de dades quan es tracti de les següents entitats:

- Els col·legis professionals i els seus consells generals.

- Els centres docents que ofereixin ensenyaments en qualsevol dels nivells establerts a la legislació reguladora del dret a l'educació, així com les universitats públiques i privades.

- Les entitats que explotin xarxes i prestin serveis de comunicacions electròniques segons el que es disposa a la seva legislació específica, quan tractin habitualment i sistemàticament dades personals a gran escala.

- Els prestadors de serveis de la societat de la informació quan elaborin a gran escala perfils dels usuaris del servei.

- Les entitats incloses a l'article 1 de la Llei 10/2014, de 26 de juny, d'ordenació, supervisió i solvència d'entitats de crèdit.

- Els establiments financers de crèdit.
- Les entitats asseguradores i reasseguradores.
- Les empreses de serveis d'inversió, regulades per la legislació del mercat de valors.
- Els distribuïdors i comercialitzadors d'energia elèctrica i els distribuïdors i comercialitzadors de gas natural.
- Les entitats responsables de fitxers comuns per a l'avaluació de la solvència patrimonial i crèdit o dels fitxers comuns per a la gestió i la prevenció del frau, incloent-hi els responsables dels fitxers regulats per la legislació de prevenció del blanqueig de capitals i del finançament del terrorisme.
- Les entitats que desenvolupin activitats de publicitat i prospecció comercial, incloent-hi les d'investigació comercial i de mercats quan portin a terme tractaments basats en les preferències dels afectats o realitzin activitats que n'impliquin l'elaboració de perfils.
- Els centres sanitaris legalment obligats al manteniment de les històries clíniques dels pacients. S'exceptuen els professionals de la salut que, malgrat estar legalment obligats al manteniment de les històries clíniques dels pacients, exerceixin l'activitat a títol individual.
- Les entitats que tinguin com un dels seus objectius l'emissió d'informes comercials que es puguin referir a persones físiques.
- Els operadors que desenvolupin l'activitat de joc per canals electrònics, informàtics, telemàtics i interactius, segons la normativa de regulació del joc.
- Les empreses de seguretat privada.
- Les federacions esportives quan tractin dades de menors d'edat.

Els responsables o encarregats del tractament no inclosos en la relació anterior poden designar de manera voluntària un delegat de protecció de dades.

8. Mesures tècniques i organitzatives

El RGPD estableix una enumeració generalista sobre les mesures que els responsables, i a vegades els encarregats, han d'aplicar per garantir que els tractaments que realitzen són conformes amb el Reglament i estar en condicions de demostrar-ho.

Quant a la metodologia de l'anàlisi de riscos que cal utilitzar, el RGPD no esmenta res. No obstant això, és lògic que les organitzacions grans o les que realitzin tractaments a gran escala utilitzin algunes de les metodologies d'anàlisi de riscos existents. No obstant això, en les organitzacions de menor grandària, sempre que no realitzin tractaments complexos, ni tractin categories especials de dades, pot ser que no sigui necessari una anàlisi formal. En qualsevol cas, en avaluar l'adequació del nivell de seguretat es tindran en compte els riscos del tractament, en particular les conseqüències de la destrucció, pèrdua o alteració accidental o il·lícita de les dades personals, i la comunicació o accés no autoritzats.

Atès que el RGPD exigeix que el RT i l'ET estiguin en disposició de demostrar que han adoptat mesures de seguretat adequades, una manera de poder demostrar-ho és mitjançant l'adhesió a codis de conducta aprovats o a alguna certificació aprovada d'acord amb el RGPD (article 32.3 RGPD).

Finalment, el RT i l'ET hauran de prendre mesures que garanteixin que qualsevol empleat amb accés a dades de caràcter personal hagi rebut la formació suficient en aquesta matèria, i que únicament té accés a aquelles dades que resulten estrictament necessàries per dur a terme la tasca que tingui encomanada.

8.1. Anàlisi de riscos

El RGPD exigeix que totes les organitzacions que tracten dades realitzin una anàlisi de risc dels seus tractaments per poder determinar quines mesures han d'aplicar i com ho han de fer.

El tipus d'anàlisi variarà en funció de:

- els tipus de tractament,
- la naturalesa de les dades,
- el nombre d'interessats afectats, i
- la quantitat i la varietat de tractaments que una mateixa organització porta a terme.

Guies de l'AEPD

L'AEPD ha desenvolupat materials per ajudar en el procés de valoració dels riscos en tractaments, com la *Guía sobre análisis de riesgos* i la *Guía de evaluaciones de impacto*, que es poden consultar en els següents enllaços <https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf> i <https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf>.

Aquestes anàlisis poden ser molt simples a entitats que porten a terme pocs tractaments i senzills que no impliquin, per exemple, dades sensibles. Però poden resultar més complexos en entitats que desenvolupin molts tractaments, que afectin un gran nombre d'interessats o que per les característiques que tenen requereixin una valoració acurada dels riscos.

8.2. Registre d'activitats de tractament (RAT)

A l'antiga LOPD 15/1999, s'establia l'obligatorietat d'elaborar un Document de Seguretat per part dels responsables dels fitxers. Aquest document havia d'identificar els fitxers i especificar les mesures tècniques i organitzatives en funció els fitxers. Aquest document havia de ser d'obligat compliment per part del personal amb accés als sistemes d'informació. Les mesures de seguretat podien ser de tipus baix, mitjà o alt. A més, existia l'obligació de notificar i registrar els fitxers que contenien dades personals davant l'autoritat de control.

Amb l'arribada del RGPD, desapareix el Document de Seguretat, igual que desapareixen els fitxers i en desapareix el registre davant l'autoritat de control. En lloc seu s'exigeix al responsable del tractament i, en el seu cas, de l'encarregat, un registre d'activitats de tractament que descrigui aquestes activitats i les mesures de seguretat aplicades. En lloc d'establir-se per nivells (alt-mitjà-baix) el RGPD estableix que aquestes mesures seran establertes en funció al risc detectat, per la qual cosa s'exigeix una anàlisi de risc prèvia al tractament.

Tenen obligació de mantenir un registre d'activitats de tractament les empreses o organitzacions a partir de 250 treballadors i també les que ocupin menys de 250 treballadors quan:

- realitzin tractaments que puguin comportar riscos per als drets o les llibertats dels interessats, quan el tractament no sigui ocasional, o
- incloguin en els tractaments categories especials de dades o dades relatives a condemnes o infraccions penals.

Tant els RT com els ET estan obligats a cooperar amb l'autoritat de control i a posar a disposició seva els registres, de manera que puguin supervisar les operacions.

El registre d'activitats de tractament o RAT ha d'incloure:

- Nom i dades de contacte del responsable i, si s'escau, del corresponsable, representant del responsable i del delegat de protecció de dades.

- Finalitats del tractament.

- Descripció de categories d'interessats i categoria de dades personals tractades.

- Descripció de categories de destinataris als quals es van comunicar o es comunicaran dades personals, així com tercers països o organitzacions internacionals.

- Transferències de dades personals a un tercer país o una organització internacional, incloent-hi la identificació del país o organització internacional i, si s'escau, la documentació de les garanties adequades.

- Terminis previstos per a la supressió de les dades, quan sigui possible.

- Descripció general de les mesures tècniques i organitzatives de seguretat.

El RAT inclou, bàsicament, la declaració de fitxers i el document de seguretat; és una fusió de tots dos (article 30.2 RGPD).

8.3. Privacitat des del disseny i per defecte

La protecció de dades des del disseny i per defecte és una qüestió d'estratègia que, tant el responsable com l'encarregat del tractament, han de tenir en consideració per assegurar el dret a la protecció de dades mitjançant l'adopció de mesures que considerin el titular de les dades personals, des del principi en què es genera una idea que pugui donar lloc a una aplicació, servei o producte. A fi de poder demostrar la conformitat amb el RGPD, el RT ha d'adoptar polítiques internes i aplicar mesures que compleixin els principis de protecció de dades des del disseny i per defecte.

La privacitat des del disseny implica que quan s'està dissenyant un producte o un servei s'ha de tenir en compte la protecció de les dades personals com un element més per prendre en consideració. Tenint en compte això últim, tant en el moment de determinar els mitjans de tractament com en el moment del tractament, el RT ha d'aplicar mesures tècniques i organitzatives apropiades (article 25.1 RGPD) per:

- protegir els drets dels interessats, com la pseudonimització de les dades que s'ha d'aplicar com més aviat millor;
- aplicar els principis de protecció de dades, com la minimització de les dades tractades;
- integrar les garanties necessàries en el tractament.

A l'hora d'implementar aquestes mesures, el RT ha de tenir en compte l'estat de la tècnica, el cost de l'aplicació, la naturalesa, l'àmbit, el context i les finalitats del tractament; avaluant els riscos que comporta el tractament per als drets i les llibertats de l'interessat.

A més, ha de garantir per defecte:

- Que únicament es tractin les dades personals necessàries per a cada una de les finalitats específiques del tractament. Una obligació que s'aplicarà a la quantitat de dades recollides, al termini de conservació i a l'accessibilitat.

- Que les dades no sigui accessibles a un nombre indeterminat de persones sense la intervenció de la persona.

- Que les funcions i el tractament siguin transparents, de manera que es permeti als interessats supervisar el tractament de dades i al RT crear i millorar elements de seguretat.

En desenvolupar, dissenyar, seleccionar o fer servir aplicacions, serveis i productes que tractin dades personals, els dissenyadors d'aquests productes haurien de tenir en compte la protecció de les dades personals, per tal que el RT pugui complir amb les obligacions que els imposa el RGPD. Un mecanisme per acreditar el compliment podria ser l'ús de certificacions d'organismes acreditats.

En tot cas, com a síntesi, els responsables han d'adoptar mesures que garanteixin que només es tractin les dades necessàries pel que fa a la quantitat de dades tractades, l'extensió del tractament, els períodes de conservació i l'accessibilitat a les dades.

8.4. Avaluació d'impacte relativa a la protecció de dades i consulta prèvia

Aquesta avaluació s'ha de realitzar amb l'assessorament del DPD (delegat de protecció de dades).

Quan sigui probable que un tractament, especialment si s'utilitzen noves tecnologies, per la seva naturalesa, abast, context o finalitats comporti un risc alt per als drets i llibertats de les persones físiques, el RT ha de realitzar una EIPD de les operacions de tractament abans de procedir a tractar les dades (article 35 RGPD). S'ha d'avaluar també l'origen, la naturalesa, la particularitat i la gravetat d'aquest risc (considerant 84 del RGPD).

Es requerirà realitzar una EIPD quan el tractament impliqui un risc alt per als drets i llibertats de les persones físiques, particularment en cas de:

- avaluació sistemàtica i exhaustiva d'aspectes personals de persones físiques, com en l'elaboració de perfils, sobre els quals es prenguin decisions que produeixin efectes jurídics per a les persones físiques o que les afectin significativament de manera similar;
- tractament a gran escala de categories especials de dades o de les dades relatives a condemnes i infraccions penals;

- control a gran escala d'una zona d'accés públic.

L'EIPD ha d'incloure com a mínim:

- La descripció detallada de:
  - descripció sistemàtica de les operacions de tractament previstes i de les finalitats de tractament i, quan procedeixi l'interès legítim del RT;
  - les diferents finalitats del tractament;
  - l'interès legítim perseguit pel responsable.

- Una avaluació de la necessitat i la proporcionalitat de les operacions de tractament respecto a la seva finalitat.

- Una avaluació dels riscos per als drets i les llibertats dels interessats.

- Les mesures previstes per afrontar els riscos, en particular les garanties, les mesures de seguretat i els mecanismes que garanteixin la protecció de dades personals.

Si una EIPD mostra un risc alt i el RT no es pot mitigar amb les mesures adequades ha de consultar l'autoritat de control abans d'efectuar el corresponent tractament de dades personals que es pretengui realitzar (article 36 RGPD).

8.5. Mesures de seguretat

Mesures de seguretat

Poden ser preventives o reactives. Sempre tenen com a última finalitat garantir la confidencialitat, la disponibilitat i la integritat de la informació (a més obstaculitzen una fuita d'informació o forat de seguretat).

L'esquema de mesures de seguretat previst en el Reglament de desenvolupament de la LOPD 15/1999 no continua sent vàlid de manera automàtica després de la data d'aplicació del RGPD. En alguns casos els responsables podran continuar aplicant les mateixes mesures que estableix el Reglament de la LOPD 15/1999 si dels resultats de l'anàlisi de riscos prèvia es conclou que les mesures són realment les més adequades per oferir un nivell de seguretat adequat. En altres ocasions serà necessari completar-les amb mesures addicionals o prescindir d'alguna de les mesures.

En tot cas, el responsable del tractament ha d'avaluar l'adequació del nivell de seguretat que cal aplicar en el tractament de dades personals, tenint en compte els riscos que presenti el tractament d'aquestes dades. El RGPD no recull ni preveu desenvolupar un catàleg de mesures de seguretat concretes, sinó que únicament en realitza una enumeració generalista.

A cada risc prèviament identificat i avaluat se li ha d'establir un control que porti a poder mesurar –i acreditar– que s'ha posat aquesta mesura de control i que funciona a fi de minimitzar la probabilitat que el risc es doni, amb el consegüent impacte associat.

D'acord amb el RGPD, l'adopció de mesures es realitzarà en funció del risc per als drets i llibertats dels interessats, tenint en compte l'estat de la tecnologia i els costos de l'aplicació, la naturalesa, abast i context del tractament. Això implica que, per determinar les mesures de seguretat aplicables, els RT hauran de realitzar una anàlisi de risc per a cada tractament que realitzi.

Des del punt de vista tècnic, les mesures engloben un conjunt d'activitats i processos destinats a evitar la sostracció, la pèrdua, la deterioració o la destrucció de dades de caràcter personal tractades. Alguns d'aquests processos poden ser:[32]

[32]Aquesta llista proporciona mesures que són aplicables i necessàries a qualsevol organització, però aquesta última n'elaborarà una llista completa en funció de les seves necessitats.

- Identificació i autenticació d'usuaris.
- Control d'accés.
- Administració d'usuaris.
- Fitxers temporals.
- Separació dels recursos de desenvolupament i producció.
- Gestió de suports i documents.
- Descartar i reutilització de suports.
- Emmagatzematge de fitxers no automatitzats.
- Custòdia de suports.
- Criteris d'arxiu.
- Seguretat en xarxes de comunicació.
- Còpies de seguretat.
- Règim de treball fora dels locals de la ubicació del fitxer.
- Trasllat de documentació.

Aquesta mena de mesures té una doble funció. Per un costat són fonamentals per acreditar que s'han assegurat raonablement les dades de caràcter personal en el cas que hi hagi una incidència. Per l'altre costat, i molt important també, permeten minimitzar l'impacte i recuperar el correcte funcionament del sistema davant una incidència real.

Les mesures de seguretat han de ser la conseqüència d'una anàlisi de riscos prèvia que determini les mesures de seguretat que resultin adequades segons la tipologia del tractament de dades personals projectat. El resultat de l'anàlisi de riscos pot recomanar les mateixes mesures que abans, recomanar noves mesures o suprimir-ne algunes que es considerin innecessàries.

Finalment, cal recordar que la LOPDGDD, per mitjà de la Disposició addicional primera relativa a les mesures de seguretat en l'àmbit del sector públic, estableix que:

«L'Esquema Nacional de Seguretat ha d'incloure les mesures que s'hagin d'implantar en cas de tractament de dades personals per evitar-ne la pèrdua, l'alteració o l'accés no autoritzat, amb l'adaptació dels criteris de determinació del risc en el tractament de les dades al que estableix l'article 32 del Reglament (UE) 2016/679.[33]

Els responsables que enumera l'article 77.1 d'aquesta Llei orgànica han d'aplicar als tractaments de dades personals les mesures de seguretat que corresponguin de les que preveu l'Esquema Nacional de Seguretat, així com impulsar un grau d'implementació de mesures equivalents en les empreses o fundacions subjectes al dret privat vinculades a aquells.

En els casos en què un tercer presti un servei en règim de concessió, encàrrec de gestió o contracte, les mesures de seguretat es corresponen amb les de l'Administració pública d'origen i s'han d'ajustar a l'Esquema Nacional de Seguretat».

(33)http://noticias.juridicas.com/base_datos/Privado/574082-regl-2016-679-ue-de-27-abr-proteccion-de-las-personas-fisicas-en-lo-que.html#I501

8.6. Notificació de violacions de seguretat de les dades

Quan es produeixi una violació de la seguretat de les dades personals, el RT l'ha de notificar a l'autoritat de control competent. La notificació s'ha de realitzar «sense dilació indeguda» i, de ser possible, dins de les 72 hores després que se n'hagi tingut constància. No és necessari notificar la violació quan sigui improbable que constitueixi un risc per als drets i les llibertats de les persones físiques (article 33 RGPD). Independentment de l'obligació de notificar-la, el RT té l'obligació de documentar qualsevol fallida en la seguretat i les mesures correctores que s'han adoptat.

Es considera que es té constància d'una violació de seguretat quan hi ha una certesa que s'ha produït i es té prou coneixement de la naturalesa i l'abast.

La mera sospita que hi ha hagut una fallida o la constatació que ha succeït algun tipus d'incident sense que se'n coneguin mínimament les circumstàncies no haurien de donar lloc, encara, a la notificació, atès que en aquestes condicions no seria possible, en la majoria dels casos, determinar fins a quin punt hi pot haver un risc per als drets i les llibertats dels interessats.

Pot haver-hi casos en què la notificació no es pugui realitzar en el termini màxim de les 72 hores.[34] En tal cas quan es notifiqui la violació de seguretat s'han d'expressar els motius de la dilació. En el cas en què no sigui possible donar tota aquesta informació en el moment de la notificació, el RGPD faculta que es pugui donar de manera gradual.

(34)Per exemple, per la complexitat a determinar-ne completament l'abast.

A més, si la violació de seguretat pot comportar un risc alt per als drets dels interessats, el RT ha de comunicar-ho sense dilació indeguda a l'interessat (article 34 RGPD).

S'entén com a violacions de seguretat o fora de seguretat tot incident que origini la destrucció, pèrdua o modificació, sigui de manera accidental o il·lícita, de dades personals, o la comunicació o accés no autoritzat a aquestes dades.

La notificació ha d'incloure un contingut mínim:

- la naturalesa de la violació de seguretat i les categories de dades i el nombre d'interessats afectats;
- les dades del delegat de protecció de dades (DPD), si s'escau;
- descripció de les possibles conseqüències de la violació;
- descripció de les mesures que s'han adoptat o proposat per arreglar la violació i mitigar-ne les conseqüències.

Documentació addicional

Guidelines on Personal data breach notification under Regulation 2016/679 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

(wp250rev.01) del WP ART.29 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

Guia forats seguretat AEPD <https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf>.

L'obligació de notificar les violacions de seguretat és un dels aspectes més controvertits del RGPD, perquè planteja moltes qüestions que el RGPD deixa sense resoldre:

- Com s'ha d'entendre el concepte de «sense dilació indeguda»?
- En quins casos no és necessària la notificació?
- Quan és probable que una violació de seguretat pugui «comportar alt risc»?
- En quins casos i com s'ha d'informar l'interessat?
- Quins elements ha de contenir la notificació?

La notificació als interessats no és necessària quan:

- El responsable hagi pres mesures tècniques o organitzatives apropiades amb anterioritat a la violació de seguretat, en concert les mesures que facin inintel·ligibles les dades per a tercers, com pot ser l'encriptat.
- El responsable hagi adoptat amb posterioritat a la fallida mesures tècniques que garanteixin que ja no hi ha possibilitat que el risc alt es materialitzi.
- La notificació suposi un esforç desproporcionat, casos en què s'han de substituir per mesures alternatives com pot ser una comunicació pública.

L'AEPD va establir en el seu moment un canal específic per notificar les fallides de seguretat en l'àmbit de les comunicacions electròniques, l'únic en què fins ara era obligatòria la notificació en aplicació de les previsions de la Directiva 2002/58 i la normativa nacional de transposició. En aquest sentit, es pot utilitzar aquest canal específic per notificar les determinades fallides de seguretat.[35]

(35)Es pot localitzar el canal de les comunicacions de les fallides de seguretat en el següent enllaç <https://sedeagpd.gob.es/sede-electronica-web/vistas/formQuiebraSeguridad/procedimientoQuiebraSeguridad.jsf>.

9. Codis de conducta i certificacions

D'acord amb el RGPD, tota empresa o organització és responsable del compliment de tots els principis de protecció de dades, així com estar en disposició de poder-ho demostrar. El RGPD proporciona eines a les empreses o organitzacions perquè puguin demostrar la seva responsabilitat. Així doncs, els responsables del tractament poden optar per realitzar la designació del delegat de protecció de dades i complementar-ho amb codis de conducta i mecanismes de certificació per demostrar el compliment dels principis de protecció de dades.

Tant el codi de conducta com la certificació són instruments voluntaris i, per tant, depèn de l'organització decidir si adopta un determinat codi de conducta o si sol·licita una certificació.

El RGPD anima els EM i les autoritats de control a promoure l'elaboració de codis de conducta com a manera de contribuir a la correcta aplicació del Reglament (article 40 RGPD).

9.1. Codis de conducta

Codis de conducta

Ja es preveien a la LOPD. S'anomenaven codis tipus de diferents sectors com el sanitari o l'assegurador.

Els codis de conducta constitueixen una mostra d'allò que es denomina autoregulació, és a dir, la capacitat de les entitats, institucions i organitzacions per regular-se a si mateixes a partir de la normativa establerta. Es poden elaborar per les associacions i altres organismes representatius de categories de responsables i encarregats, per als quals seran vinculants un cop s'hagin adherit als codis de conducta.

Tal com estableix la mateixa AEPD, els codis de conducta, a diferència de les certificacions, ja estaven previstos d'una forma genèrica a la Directiva 95/46/CE i, en el cas d'Espanya, es va adaptar al dret nacional tant a la LORTAD com a la LOPD. Aquest marc normatiu ha propiciat l'elaboració de catorze codis tipus en l'àmbit del sector privat i dos en l'àmbit del sector públic com a mecanismes d'autoregulació en matèria de protecció de dades, complementant el marc regulador que existent.

Tenen per objecte especificar l'aplicació de les obligacions que estableix el RGPD, en particular respecte als principis del tractament, la legitimitat, la informació que s'ha de facilitar als interessats, l'exercici dels drets dels interessats, les mesures de seguretat aplicables, etc. (article 40.2 RGPD). El mateix codi ha d'establir els mecanismes de control del seu compliment per part dels RT que s'hagin compromès a aplicar-lo, sense perjudici de la facultat de supervisió

que posseeix l'autoritat competent o la que s'atribueix a un organisme acreditat (article 41 RGPD). Constitueixen una eina útil per demostrar l'adequació de l'organització adherida a les obligacions que el RGPD li imposa.

Tal com estableix l'ens espanyol, en relació amb els codis de conducta, i segons s'estableix als articles 40 i 41 del Reglament (UE) 2016/679 (RGPD) i l'article 38 de la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD), aquests codis es podran promoure, a més de per associacions o altres organismes que representin categories de responsables o encarregats de tractament, per empreses o grups d'empreses, així com per les Administracions Públiques i les entitats que pertanyin al sector públic.

Així mateix, a la LOPDGDD, es preveu que es pot promoure l'adopció de codis de conducta pels organismes o entitats que assumissin les funcions de supervisió i resolució extrajudicial de conflictes als quals es refereix l'article 41 del RGPD.

Els codis de conducta especifiquen l'aplicació del Reglament a les característiques i les necessitats dels diferents sectors d'activitat pel que fa a:

- el tractament lleial i transparent;
- els interessos legítims que persegueixen els responsables del tractament en contextos específics;
- la recollida de dades personals;
- la pseudonimització de dades personals;
- la informació que es proporciona al públic i als interessats;
- l'exercici dels drets dels interessats;
- la informació que es proporciona als infants i la protecció que se'ls dona, així com la manera d'obtenir el consentiment dels titulars de la pàtria potestat o tutela sobre l'infant;
- les mesures i els procediments als quals es refereixen els articles 24 i 25 i les mesures per garantir la seguretat del tractament al qual es refereix l'article 32;
- la notificació de violacions de la seguretat de les dades personals a les autoritats de control i la comunicació d'aquestes violacions als interessats;

- la transferència de dades personals a tercers països o organitzacions internacionals, o

- els procediments extrajudicials i altres procediments de resolució de conflictes que permetin resoldre les controvèrsies entre els responsables del tractament i els interessats relatives al tractament, sense perjudici dels drets dels interessats en virtut dels articles 77 i 79 del Reglament de protecció de dades personals.

Quan una associació o organisme representatiu d'un sector o un grup de responsables de tractament es disposi a crear un codi de conducta (o a modificar-lo) han de presentar un projecte a l'autoritat de control competent. Després de comprovar-ne l'adequació a la normativa, l'autoritat de control ha d'emetre un dictamen sobre la conformitat del codi amb el RGPD i l'aprova si considera que ofereix suficients garanties. Si el codi s'aprova s'ha de procedir a registrar-lo i publicar-lo. Un codi de conducta pot ser validat a tota la Unió Europea mitjançant un acte d'execució de la Comissió. El Comitè ha d'arxivar en un registre tots els codis de conducta, les modificacions i les ampliacions que s'aprovin, i els ha de posar a disposició pública per qualsevol mitjà apropiat.

Figura 6. Esquema de les entitats de certificació

Per què entitats de certificació? Perquè la persona responsable de les dades ha de tenir els coneixements «validats».

International Acreditation Forum	Internacional.
Organisme acreditador	Un per país.
Entitats certificadores, organismes de certificació	Molt poques i fan els exàmens perquè algunes persones puguin obtenir la certificació.
Entitats de formació	Centres que imparteixen formació per presentar-se als exàmens i obtenir la certificació.
Persones certificades	A la pràctica DPD/DPO.

Font: elaboració pròpia.

Els codis de conducta i les certificacions constitueixen instruments que faciliten poder demostrar que es compleixen amb el RGPD, particularment en relació amb la identificació i l'avaluació del risc que suposa el tractament, així com amb l'adopció de bones pràctiques per mitigar el risc identificat. A més, permeten avaluar ràpidament el nivell de protecció d'una empresa.

9.2. Certificacions

De la mateixa manera que els codis de conducta, els certificats, els segells i les marques de protecció de dades faciliten poder demostrar que el responsable o l'encarregat de tractament compleix amb el RGPD. No obstant això, tenir una certificat no limita la responsabilitat del RT o de l'ET (article 42.4 RGPD), però facilita poder provar el compliment de la normativa, a més del fet que el certificat contribueix a augmentar la transparència, ja que l'interessat pot avaluar de manera ràpida i eficaç el nivell de protecció que ofereix el RT o l'ET.

El certificat és voluntari (article 42.3 RGPD) i només pot ser expedit per un organisme de certificació autoritzat (article 43 RGPD) o per l'autoritat de control competent basant-se en els criteris que aprovin les autoritats o el Comitè Europeu de Protecció de Dades.

Una organització pot adoptar un mecanisme de certificació aplicat per un dels organismes de certificació que hagi rebut l'acreditació d'una APD o un organisme d'acreditació nacional o tots dos, segons el que estableixi la legislació de cada estat membre.

10. Transferències internacionals de dades

Aquest concepte és molt rellevant en protecció de dades en un context de societat digital globalitzada en què, de manera habitual, s'utilitzen eines que emmagatzemen dades personals que se situen en països de fora de la Unió Europea. És el cas d'eines com el màrqueting per correu electrònic, analítiques o fins i tot xarxes socials.

S'entén per transferència internacional de dades (TID) la transmissió de dades personals des de l'Espai Econòmic Europeu (EEE), és a dir, els països de la UE i Liechtenstein, Islàndia i Noruega a altres països fora de la Unió Europea.

Exemple de transferència internacional de dades

Si teniu un simple blog amb un *hosting* situat als EUA, els comentaris (que s'emmagatzemen a la base de dades de WordPress) són una transferència internacional de dades als EUA, perquè s'envien i s'emmagatzemen en un servidor als EUA. Per la mateixa lògica, si el vostre *hosting* és espanyol, no ho són.

Una de les novetats que introdueix el Reglament respecte a la regulació anterior de les TID és la possibilitat que l'encarregat de tractament pugui realitzar TID. Transferir dades personals des d'un país de la UE a un país fora de l'EEE només és possible quan:

- Hi ha una decisió d'adequació emesa per part de la Comissió Europea.

- Si no hi ha decisió d'adequació, s'ofereixen garanties adequades. Aquestes garanties adequades poden ser aportades, sense necessitats d'autorització de l'autoritat de control per:
  - un instrument jurídicament vinculant i exigible entre les autoritats o organismes públics;
  - normes corporatives vinculants de conformitat amb l'article 47;
  - clàusules tipus de protecció de dades adoptades per la Comissió de conformitat amb el procediment d'examen al qual es refereix l'article 93, apartat 2;
  - clàusules tipus de protecció de dades adoptades per una autoritat de control i aprovades per la Comissió d'acord amb el procediment d'examen que es refereix a l'article 93, apartat 2;
  - un codi de conducta aprovat d'acord amb l'article 40, juntament amb compromisos vinculants i exigibles del responsable o l'encarregat del

tractament al tercer país d'aplicar garanties adequades, incloses les que fan referència als drets dels interessats, o

– un mecanisme de certificació aprovat d'acord amb l'article 42, juntament amb compromisos vinculants i exigibles del responsable o l'encarregat del tractament al tercer país d'aplicar garanties adequades, incloses les que fan referència als drets dels interessats.

10.1. El sistema de decisions d'adequació

La Comissió Europea manté una llista de tercers països, territoris, un sector específic d'un país o una organització internacional fora de l'EEE que ofereixen un nivell adequat de protecció per a les dades personals (article 42). En aquest cas les transferències de dades no requereixen l'autorització específica de l'AEPD. El RGPD introdueix l'obligació de revisar de manera periòdica, com a mínim cada quatre anys, la decisió d'adequació per part de la Comissió.[36]

[36]Para saber els països que ofereixen un nivell adequat de protecció ho podeu consultar aquí <https://ec.europa.eu/info/law/law-topic/data-protection_en>.

Així mateix, tal com ha recordat la mateixa AEPD, en el cas que la transferència internacional de dades amb destinació a un d'aquests països sigui conseqüència d'una prestació de serveis, aquesta circumstància no eximeix de l'obligació d'haver de subscriure un contracte de prestació de serveis per tercer (encarregat del tractament) conforme al que es disposa a l'article 28 del RGPD.

En tot cas, la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD) estableix a l'article 42 els supòsits sotmesos a autorització prèvia de les autoritats de protecció de dades.

10.2. *Privacy Shield*

La Sentència del Tribunal de Justícia (Gran Sala) de 16 de juliol de 2020, (Assumpte C-311/18) va anul·lar la Decisió 2016/1250 de la Comissió que declarava el nivell adequat de protecció de l'esquema de l'Escut de Privacitat (*Privacy Shield*) per a les transferències internacionals de dades als EUA. No obstant això, la STJUE reconeix la validesa de les clàusules contractuals estàndard adoptades per la Comissió Europea per realitzar transferències internacionals de dades entre un RT establert a la UE i un ET fora de la UE.

Bibliografia complementària

Per saber més sobre el *Privacy Shield* consulteu *Guide to the EU-US Privacy Shield* <https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf>.

Aquest *Escut de Privacitat* és un acord entre les autoritats dels EUA i les europees, en què s'estableix una col·laboració mútua i estan obligades a publicar normes específiques sobre el tractament de les dades que recopilen. Això també implica que els governs dels estats implicats no poden accedir de manera indiscriminada a les dades personals, sinó que únicament ho poden fer quan sigui imprescindible i comptant amb les garanties pertinents.[37]

[37]Consulteu la *Guía acerca del Escudo de Privacidad EE. UU-UE.* <https://www.aepd.es/sites/default/files/2019-09/guia-acerca-del-escudo-de-privacidad.pdf>.

L'EU-US *Privacy Shield* va ser adoptat el juliol de 2016 per la Comissió Europea mitjançant la Decisió (UE) 2016/1250 de 12 de juliol de 2016. A la pàgina web de l'Escut de Privacitat s'accedeix a la relació de les entitats certificades.[38] L'Escut de Privacitat ofereix una sèrie de drets i obliga les empreses a protegir les dades personals d'acord amb els «principis de privacitat».

(38)https://www.privacyshield.gov/list

10.3. Normes corporatives vinculants (*Binding Corporate Rules*)

La BCR són un conjunt de regles o clàusules corporatives vinculants que tenen per objecte establir les pràctiques que una entitat duu a terme en matèria de tractament de dades de caràcter personal amb la finalitat de facilitar les transferències internacionals de dades en el si d'aquesta corporació. Les BCR constitueixen un instrument que els grups multinacionals poden fer valer davant les autoritats de protecció de dades, per garantir la legalitat de les operacions de transferència de dades en l'organització, independentment que el país de destinació garanteixi o no un «nivell adequat de protecció» conforme a la normativa vigent al país d'origen de les dades (article 41). Han de tenir un contingut mínim i ser aprovades per l'autoritat de control competent (en el cas d'Espanya, principalment l'AEPD) de conformitat amb el mecanisme de coherència establert a l'article 63 del RGPD.

Aquestes normes corporatives vinculants únicament faculten per a les TID dins del mateix grup d'empreses, però en cap cas faculten per realitzar TID fora del grup.[39]

(39)Per consultar la llista d'empreses europees que han optat per aquest sistema. <https://ec.europa.eu/info/law/law-topic/data-protection_en>.

10.4. Excepcions

Es preveu la possibilitat de realitzar transferències en determinades circumstàncies sense necessitat d'aportar garanties adequades (article 43). La relació d'excepcions recull diversos supòsits, que s'especifiquen a l'article 49.1 del Reglament (UE) 2016/679.

- L'interessat ha donat el consentiment explícit després que se l'hagi informat dels riscos que li comporta la TID.
- La TID sigui necessària per a l'execució d'un contracte entre l'interessat i el RT o per l'execució de mesures contractuals sol·licitades pel mateix interessat.
- La TID sigui necessària per a l'execució, la celebració o l'execució d'un contracte en interès de l'interessat, entre el RT i un tercer.
- Per raons d'interès públic, per a l'exercici o la defensa de reclamacions.

Bibliografia complementària

Més informació a *EDPB Guidelines* <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf>.

- Per protegir els interessos vitals de l'interessat quan es trobi incapacitat per donar el consentiment.

- Quan s'acrediti un interès legítim i la TID es realitzi des d'un registre públic que estigui obert a la consulta del públic en general, que no ha d'incloure la totalitat de les dades que es trobin en el registre.

Encara que no es pogués complir cap dels supòsits esmentats, encara seria possible un supòsit concret en què el RT podria realitzar una TID. En efecte, el RGPD introdueix una novetat respecte a la normativa anterior, la possibilitat de realitzar una TID basada en l'interès legítim imperiós que persegueix el RT. Perquè sigui possible la TID no ha de ser repetitiva, ha d'afectar només un nombre limitat d'interessats, ser necessària per aconseguir els interessos legítims imperiosos del RT i no han de prevaler els drets i llibertats de l'interessat. El RT ha d'aportar garanties adequades després d'avaluar totes les circumstàncies concurrents. Si es compleixen totes aquestes condicions el RT ha d'informar l'autoritat de control (AEPD) de la TID i els interessats facilitant-los tota la informació preceptiva i informant-los dels interessos legítims imperiosos que es persegueixen (article 47.1 RGPD).

11. Les autoritats de control i el règim sancionador

11.1. Les autoritats de control

Cada EM ha d'establir autoritats de control (AC) capacitades per exercir les funcions i les competències amb independència. En funció de l'estructura constitucional, organitzativa i administrativa, els EM podran tenir una o més AC. En virtut de l'anterior, fins avui en l'Estat espanyol s'han creat quatre AC: l'Agència Espanyola de Protecció de Dades (AEPD);[40] l'Autoritat Catalana de Protecció de Dades (APDCAT);[41] l'Agència Basca de Protecció de Dades (AVPD);[42] i el Consell de Transparència d'Andalusia.[43] Cada AC és competent en el territori de l'EM per exercir els poders i les funcions que el Reglament els confereix. A l'Estat espanyol les AC autonòmiques són competents per exercir els seus poders i funcions en l'àmbit del territori de la comunitat autònoma, limitada a l'àmbit de les seves competències. En canvi, l'AEPD exerceix els seus poders i funcions a tot el territori de l'Estat respecte als tractaments realitzats per les AAPP de l'Estat (també a la resta d'autonomies que no han desplegat competències en la matèria) i altres organismes públics i privats, així com de particulars i empreses.

(40) https://www.aepd.es/

(41) http://apdcat.gencat.cat/es/inici/

(42) http://www.avpd.euskadi.eus/s04-5213/es

(43) https://www.juntadeandalucia.es/transparencia/transparencia-andalucia/consejo-transparencia.html

Totes les AC s'han de dotar dels recursos financers i humans necessaris per realitzar les funcions amb eficàcia. Els membres de les AC han de ser nomenats mitjançant procediments transparents pel Parlament, el Govern o el cap de l'EM. En el cas de l'AEPD, el Govern espanyol designa el director o directora de l'Agència mitjançant decret, tal com s'estableix en l'articulat de la LOPDGDD.

Les AC exerceixen funcions de supervisió, assessorament, consultives, de sensibilització dels ciutadans, etc. (article 57 RGPD).

Per poder exercir les funcions les AC es doten de poders (article 58 RGPD):

- de recerca: per exemple, ordenar el RT o ET que li facilitin la informació que es requereix;
- correctius: sancionar amb una advertència o amb una prevenció la possibilitat d'infracció o la infracció del Reglament, etc.;
- d'autorització i consultius: aprovar normes corporatives vinculants, emetre dictàmens sobre assumptes relacionats amb la protecció de dades, etc.

11.2. El règim sancionador

El règim sancionador

Articles 77 a 84 GDPR.

El RGPD estableix un règim sancionador flexible. Al costat de les sancions econòmiques, el RGPD també preveu l'aplicació d'altres accions correctives (article 83 RGPD).

- Les sancions econòmiques han de ser efectives, proporcionades i dissuasives, i poden arribar fins a un màxim de 20.000.000 euros o, si es tracta d'una empresa, a la quantitat equivalent al 4 % del volum de negoci anual de l'empresa (el que resulti més alt). A priori són xifres astronòmiques, tot i que el Reglament ofereix diferents criteris de modulació.

- Les accions correctives inclouen advertències, prevencions, ordres d'adaptació de tractaments, limitacions temporals o definitives de tractaments, inclosa la prohibició, etc.

Les multes administratives (sancions) s'han d'imposar en funció de les circumstàncies de cada cas individual i han de ser efectives, proporcionades i dissuasives. En decidir la imposició d'una multa administrativa i la quantia en cada cas individual s'han de tenir degudament un conjunt d'aspectes definits a l'article 83 del RGPD. El rang de sancions segons la importància que tenen és ara:

- Sancions lleus: no estableix un rang mínim de quantia.

- Sancions greus: multa administrativa de fins a 10.000.000 euros o, en el cas d'empreses, de quantia equivalent al 2 % com a màxim del volum de negoci total anual global de l'exercici financer anterior, la quantia que resulti més alta.

- Sancions molt greus: multa administrativa de fins a 20.000.000 euros o, en el cas d'empreses, de quantia equivalent al 4 % com a màxim del volum de negoci total anual global de l'exercici financer anterior, la quantia que resulti més alta.

Qualsevol interessat que hagi patit un perjudici, material o immaterial, a conseqüència d'una operació de tractament que no s'atingui a la normativa de protecció de dades, té la potestat de presentar una reclamació davant l'Autoritat de Control corresponent i, si escau, pot requerir una indemnització si es demostra que els seus drets s'han vist vulnerats. L'interessat ara té dret a reclamar, a la tutela judicial i a una indemnització.

L'incompliment per part d'una organització pot comportar sancions, indemnitzacions i altres accions correctives simultàniament.

12. Tractaments específics de dades personals

Es poden escollir molts exemples de tractaments especials: tractaments de dades relacionats amb comunicacions electròniques, finalitats de màrqueting, solvència patrimonial i crèdit o bé de salut. Entre aquests últims s'ha escollit el que està relacionat amb la COVID-19.

12.1. Tractaments de dades derivats de la situació de la COVID-19

L'11 de març del 2020 l'Organització Mundial de la Salut va declarar pandèmia internacional la situació d'emergència ocasionada pel brot epidèmic de COVID-19. El Govern, en la reunió extraordinària del Consell de Ministres de 14 de març del 2020, va aprovar el Reial decret 463/2020, de 14 de març, pel qual es declara l'estat d'alarma per a la gestió de la situació de crisi sanitària ocasionada per la COVID-19.

Prenent com a base les dades disponibles i els informes d'avaluació elaborats per les autoritats competents delegades durant aquest període, el Govern va concloure que la situació d'emergència sanitària generada pel brot epidèmic de COVID-19 no se superaria en el termini previst inicialment pel Reial decret 463/2020, de 14 de març, per la qual cosa van succeir diferents pròrrogues per intentar frenar l'avançament de la pandèmia.

El 28 d'abril del 2020, el Govern va anunciar l'inici del pla per a la transició cap a una nova normalitat, i a conseqüència, multitud d'organitzacions van iniciar una sèrie d'actuacions preventives orientades a garantir un nivell de protecció adequat respecte dels seus treballadors o qualssevol tercers que s'hi relacionin, per unir forces contra l'avançament de la pandèmia originada per la COVID-19.

Adoptar aquestes actuacions va suposar la producció de múltiples impactes per als drets i llibertats dels treballadors, clients o qualssevol tercers que es relacionessin amb aquestes organitzacions. Un dels possibles impactes s'estableix en matèria de protecció de dades de caràcter personal, on s'ha de prestar especial cautela en el moment de dur a terme algunes actuacions, que s'han de realitzar respectant el que es disposa al Reglament (UE) 2016/679, General de Protecció de Dades i la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

En aquest context, es van produir diferents pronunciaments per part de les autoritats europees i espanyoles amb competències sobre la matèria, que van voler posar llum sobre algunes qüestions que generaven una certa incertesa.

D'una banda, les autoritats europees van emetre diversos pronunciaments, entre els quals es pot destacar principalment el que és d'interès aquí, les consideracions publicades per part del Comitè Europeu de Protecció de Dades. Concretament les Directrius 03/2020 sobre el processament de dades que fan referència a la salut amb finalitats de recerca científica en el context del brot de COVID-19 i les Directrius 04/2020 sobre la utilització de dades de localització i eines de rastreig de contactes en el context del brot de COVID-19, les quals adopten un enfocament similar establint que les normes de protecció de dades no obstaculitzen les mesures adoptades per lluitar contra la crisi sanitària de COVID-19, sempre que els responsables del tractament garanteixin la protecció de les dades personals que s'hagin obtingut.

Els documents referits van establir una sèrie d'obligacions per al tractament de dades en situacions específiques. Les Directrius sobre el tractament de dades sanitàries amb finalitats de recerca científica afirmaven que els responsables del tractament havien de basar els tractaments en alguna de les bases legals establertes a l'article 6 del RGPD per al tractament de les dades obtingudes (per exemple, el consentiment o l'interès legítim), a més de comptar amb alguna de les excepcions aplicables a la prohibició de tractament de dades relatives a la salut en relació amb l'interès públic, en particular en l'àmbit de la salut pública, la recerca científica o les finalitats estadístiques (en virtut de l'article 9, apartats i i j).

A les Directrius sobre la utilització de dades de localització i rastreig de contactes s'establia que en aquest context s'ha de prioritzar el tractament de les dades personals d'una manera anonimitzada, encara que el consentiment de l'afectat pugui ser una base de legitimació suficient quan les dades de localització obtingudes no resultin anonimitzades. I en tot cas, l'EDPB també va recordar que quan es realitzen tractaments en relació amb la vigilància sistemàtica o l'ús de dades a gran escala, s'han de dur a terme les corresponents avaluacions d'impacte sobre protecció de dades (EIPD), i recomana fins i tot publicar-les.

Agència Espanyola de Protecció de Dades

Cada un dels documents als quals es fa referència en els punts 1 a 4 es poden consultar respectivament als següents enllaços:

1)https://www.aepd.es/es/documento/2020-0017.pdf

2)https://www.aepd.es/sites/default/files/2020-03/FAQ-COVID_19.pdf

3)https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos

4)https://www.aepd.es/media/guias/nota-tecnica-proteger-datos-teletrabajo.pdf

D'altra banda, l'AEPD va efectuar diverses publicacions per intentar donar resposta a aquests dubtes, entre les més importants es poden destacar les següents:

1) Informe en què analitza el tractament de dades personals en relació amb la situació derivada de l'extensió del virus de la COVID-19.[44]

[44]Es pot consultar al següent enllaç <https://www.aepd.es/es/documento/2020-0017.pdf> (12 de març del 2020).

El document recull, entre altres consideracions, que el RGPD estableix explícitament al considerant 46 com a base jurídica per al tractament lícit de dades personals en casos excepcionals, com el control d'epidèmies i la seva propagació, la **missió realitzada en interès públic** (article 6.1.e) o els **interessos vitals de l'interessat o altres persones físiques** (article 6.1.d), sense perjudici que hi pugui haver altres bases com, per exemple, el compliment d'una obligació legal (per a l'ocupador en la prevenció de riscos laborals del seu personal). Aquestes bases jurídiques **permeten el tractament de dades sense consentiment dels afectats**.

2) Preguntes freqüents dirigides tant a ciutadans com a empreses i altres subjectes obligats al compliment de la normativa de protecció de dades.

3) Comunicat en relació amb la presa de temperatura per part de comerços, centres de treball i altres establiments, en què es recomana una anàlisi específica sobre la proporcionalitat de la mesura.

4) L'Agència va emetre un seguit de **recomanacions** per a les situacions de mobilitat i teletreball, que instaven les empreses sobre la necessitat d'informar els teletreballadors sobre les mesures de seguretat i precaució que han de prendre en el desenvolupament de les funcions laborals, així com del respecte dels drets d'intimitat o desconnexió digital.

Resum

«La protecció de les persones físiques en relació amb el tractament de dades personals és un dret fonamental [...]».[45]

(45)Considerant 1 GDPR.

Les noves tecnologies de transmissió i de tractament d'informació han comportat una dispersió elevada de les dades personals. A més, la diversitat d'informació que es pot associar a una persona és àmplia. Les dades que es consideren personals s'utilitzen per a moltes activitats quotidianes. Per això els estats, cada vegada més conscients de la situació, busquen regular (amb lleis) les diferents situacions en què s'han de protegir les dades. Davant un món globalitzat, aquestes normes ja no poden ser solament de caràcter nacional, sinó que han de transcendir les fronteres.

Així doncs, el reglament general de protecció de dades és una normativa en l'àmbit de la Unió Europea, per la qual cosa qualsevol empresa de la Unió, o aquelles empreses que tinguin negocis a la Unió Europea, que manegin informació personal (es dirigeixin a ciutadans de la UE) de qualsevol mena tenen l'obligació d'adoptar aquelles mesures que assegurin raonablement que, a priori, estan en condicions de complir amb els principis, garanties i drets que s'estableixen al Reglament.

El fonament d'aquest reglament és **assegurar i acreditar la protecció de les dades.** Per això, a més del compliment, l'organització ha d'estar en condicions de demostrar les mesures de seguretat aplicades si es donés el cas i **acreditar** que es compleix el Reglament. L'objectiu és evitar així els riscos de diversa probabilitat i gravetat per als drets fonamentals dels usuaris.

En termes pràctics, aquest principi requereix que les organitzacions analitzin quines dades tracten, amb quines finalitats i quina mena d'operacions de tractament duen a terme. A partir d'aquest coneixement han de determinar la forma en què aplicaran les mesures que el GDPR preveu, assegurant-se que aquestes mesures són les més adequades i que ho poden demostrar davant els interessats i les autoritats en una supervisió. L'objectiu és evitar als titulars de les dades uns danys que a posteriori poden ser molt difícils o impossibles de reparar.

En síntesi, el GDPR exigeix una **actitud conscient, diligent i proactiva** del tractament de les dades que es duguin a terme.

Hi ha un canvi important respecte a la llei anterior (Llei orgànica de Protecció de Dades, LOPD de 1999) que principalment buscava evitar la vulneració dels drets dels interessats. El GDPR mira d'anticipar-se a la infracció o lesió de drets, establint el principi de responsabilitat proactiva, tot i que també estableix sancions importants quan no es compleixi amb la normativa.

És evident que el ciutadà cada vegada és més conscient de les seves dades i els drets que s'hi associen i cada vegada serà més exigent amb les empreses i professionals que les gestionen.

Glossari

AC *f* Vegeu **autoritat de control**.

accés autoritzat *m* Autoritzacions concedides a un usuari per utilitzar els diversos recursos. En aquest cas inclouen les autoritzacions o funcions que s'atribueixin a un usuari per delegació del responsable del fitxer o tractament o del responsable de seguretat.

AEPD *f* Agència Espanyola de Protecció de Dades.

afectat *m i f* Persona física titular de les dades que siguin objecte de tractament. Tal com detalla el nou reglament, l'afectat disposa d'un seguit de drets com el dret a la informació sobre la identitat del responsable de les dades i les finalitats del tractament, entre altres.
sin. **interessat** i **titular de les dades**

autoritat de control *f* L'autoritat pública independent establerta per un estat membre segons allò que es disposa a l'article 51 de RGPD.
sigla **AC**

backup *m* Vegeu **còpia de seguretat**.

categoria especial de dades *f* Dades que revelin l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques, o l'afiliació sindical, les dades genètiques, les dades biomètriques dirigides a identificar de manera unívoca una persona física, dades relatives a la salut o dades relatives a la vida sexual o a les orientacions sexuals (article 9 de la Llei).

consentiment de l'interessat *m* Tota manifestació de voluntat lliure, específica, informada i inequívoca per la qual l'interessat accepta, sigui amb una declaració o una clara acció afirmativa, el tractament de dades personals que l'afecten.

còpia de seguretat *f* Còpia de les dades d'un fitxer automatitzat en un suport que en possibiliti la recuperació.
en backup

dada biomètrica *f* Dades personals obtingudes a partir d'un tractament tècnic específic, relatives a les característiques físiques, fisiològiques o conductuals d'una persona física que permetin o confirmin la identificació única d'aquesta persona, com ara imatges facials o dades dactiloscòpiques. El RGPD aclareix que el tractament de fotografies no s'ha de considerar sistemàticament tractament de categories especials de dades personals. Únicament es consideren dades biomètriques quan el fet de ser tractades amb mitjans tècnics específics permeti la identificació o l'autenticació unívoques d'una persona física.

dada de caràcter personal *f* Qualsevol dada que concerneixi persones físiques identificades o identificables.

dada genètica *f* Dades personals relatives a les característiques genètiques heretades o adquirides d'una persona física que proporcionin una informació única sobre la fisiologia o la salut d'aquesta persona, obtingudes en particular de l'anàlisi d'una mostra biològica d'aquesta persona.

dada personal *f* Tota informació sobre una persona física identificada o identificable («l'interessat»). Es considera persona física identificable tota persona la identitat de la qual es pugui determinar, directament o indirecta, 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.

dada relativa a la salut *f* Dades relatives a la salut física o mental d'una persona física, inclosa la prestació de serveis d'atenció sanitària, que revelin informació sobre el seu estat de salut. Entre altres: la informació recollida en la inscripció a l'efecte de la prestació d'assistència sanitària, la recollida amb prestació de tal assistència; tot número, símbol o dada assignada a una persona que la identifiqui de manera unívoca a efectes sanitaris; la informació obtinguda de proves o exàmens, inclosa la procedent de dades genètiques i mostres biològiques; i qualsevol informació relativa a una malaltia, discapacitat, risc de patir malalties; l'historial mèdic, el tractament clínic o l'estat fisiològic o biomèdic de l'interessat, independentment de la seva font.

destinatari *m i f* Persona física o jurídica, autoritat pública, servei o un altre organisme al qual es comuniquin les dades, es tracti o no d'un tercer. No obstant això, no es conside-

ren destinataris les autoritats públiques que puguin rebre dades personals en el marc d'una recerca concreta d'acord amb el Dret de la UE o dels EM.

elaboració de perfils *f* Tota forma de tractament automatitzat de dades personals que consisteixi a utilitzar dades personals per avaluar determinats aspectes personals d'una persona física, en particular per analitzar o predir aspectes relatius al rendiment professional, la situació econòmica, la salut, les preferències personals, els interessos, la fiabilitat, el comportament, la ubicació o els moviments d'aquesta persona física.

EM *m* Estat membre de la UE.

encarregat de tractament *m i f* Persona física o jurídica, autoritat pública, servei o un altre organisme que tracti dades per compte del responsable del tractament.

fitxer *m* Tot conjunt organitzat de dades de caràcter personal, sigui quina sigui la forma o modalitat de la seva creació, emmagatzematge, organització i accés.

fitxer temporal *m* Fitxers de treball creats per usuaris o processos que són necessaris per a un tractament ocasional o com a pas intermedi durant la realització d'un tractament.

forat de seguretat *m* Vegeu **violació de la seguretat de les dades personals**.

interessat *m i f*
sin. **afectat** i **titular de les dades**

Llei orgànica 3/2018 *f* De 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals o «LOPDGDD» indistintament.

limitació del tractament *f* Marcatge de les dades de caràcter personal conservades per limitar-ne el tractament en el futur.

norma corporativa vinculant *f* Les polítiques de protecció de dades personals assumides per un responsable o encarregat del tractament establert en el territori d'un estat membre per a transferències o un conjunt de transferències de dades personals a un responsable o encarregat en un o més països tercers, dins d'un grup empresarial o una unió d'empreses dedicades a una activitat econòmica conjunta.

persona identificable *m i f* Tota persona la identitat de la qual es pugui determinar directament o indirecta mitjançant qualsevol informació referida a la seva identitat física, fisiològica, psíquica, econòmica, cultural o social.

pseudonimització *f* El tractament de dades personals de manera que ja no es puguin atribuir a l'interessat sense fer servir 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.

Reglament *m* (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. Els termes reglament, RGPD, fan al·lusió a aquest cos normatiu, del qual es pot consultar el text íntegre en aquest enllaç <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&ffrom=ES>.

responsable de tractament *m i f* Persona física o jurídica, autoritat pública, servei o un altre organisme que, sol o juntament amb altres, determini les finalitats i els mitjans del tractament.

responsable de seguretat *m i f* Persona o persones a les quals el responsable del fitxer ha assignat formalment la funció de coordinar i controlar les mesures de seguretat aplicables.

sistema d'informació *m* Conjunt de fitxers, tractaments, programes, suports, i si escau, equips emprats pel tractament de dades de caràcter personal.

sistema de tractament *m* Manera en què s'organitza o s'utilitza un sistema d'informació. Tenint en compte el sistema de tractament els sistemes d'informació poden ser automatitzats, no automatitzats o parcialment automatitzats.

tercer *m i f* Persona física o jurídica, pública o privada, o òrgan administratiu diferent de l'afectat o 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 del tractament o de l'encarregat del tractament.

titular de les dades *m i f*
sin. **afectat** i **interessat**.

transferència internacional de dades *f* Tractament de dades que suposa una transmissió de dades fora del territori de l'Espai Econòmic Europeu, o bé constitueixi una cessió o comunicació de dades, o bé tingui per objecte la realització d'un tractament de dades per compte del responsable del fitxer establert en territori espanyol.

tractament *m* Qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, sigui per procediments automatitzats o no, com la recollida, registre, organització, estructuració o conservació, adaptació o modificació, extracció, consulta, utilització, comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció.

tractament de dades *m* Operacions i procediments tècnics de caràcter automatitzat o no, que permetin la recollida, gravació, conservació, modificació, bloqueig i cancel·lació, així com les cessions de dades que resultin de comunicacions, consultes, interconnexions i transferències.

violació de la seguretat de les dades personals *f* Tota violació de la seguretat que ocasioni la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra forma, o la comunicació o accés no autoritzats a aquestes dades.

Bibliografia

Doctrina

Aberasturi Gorriño, U. (2013). «El derecho a la indemnización en el artículo 19 de la Ley orgánica de protección de datos de carácter personal». *Revista Aragonesa de Administración Pública* (núm. 41-42).

Álvarez Hernando, J. (2017). «El Reglamento Europeo y la futura Ley General de Protección de Datos: sus principales novedades». *Aranzadi digital* (núm. 1).

Alzaga Villaamil, O. (2017). *Comentario sistemático a la Constitución española de 1978*. Madrid: Marcial Pons.

Andreu Martínez, M. B. (2013). *La protección de datos personales de los menores de edad*. Navarra: Aranzadi.

Aparicio Salom, J. (2002). *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*. Navarra: Aranzadi.

Arenas Ramiro, M. (2006). *El derecho fundamental a la protección de datos personales en Europa*. València: Tirant lo Blanch.

De Miguel Asensio, P. (2015, gener). «Protección de Datos Personales». A: *Estudios y Comentarios legislativos*.

De la Hera Justicia, Z. (2017). «El Reglamento General de Protección de Datos y su incidencia en la administración local». *La Administración práctica* (núm. 3).

Gonzalez Calvo, M. (2018). «La nueva figura del Delegado de Protección de Datos». *Actualidad Jurídica Aranzadi* (núm. 939).

Guerrero Picó, M.ª C. (2006). *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*. Navarra: Thomson-Reuters «Civitas».

Guichot Reina, E. (2014). «Transparencia, Acceso a la Información Pública y Buen Gobierno: Estudio de la Ley 19/2013». *Revista de Estudios de la Administración Local y Autonómica: Nueva Época* (núm. 2).

Lucas Murillo De la cueva, P. (1996). «Las funciones de la Agencia de Protección de Datos». *Jornadas sobre el Derecho Español de la Protección de Datos Personales*. Madrid: Agència de Protecció de Dades.

Lucas Murillo De la Cueva, P. (2009). *El derecho a la autodeterminación informativa*. Madrid: Fundació Col·loqui Jurídic Europeu.

Lesmes Serrano, C. (2007). *La ley de protección de datos. Análisis y comentario de su jurisprudencia*. Valladolid: Lex Nova.

Martínez Martínez, R. (2004). *Una aproximación crítica a la autodeterminación informativa*. Madrid: Civitas.

Martínez Martínez, R. (2007). «El derecho fundamental a la protección de datos: perspectivas». *Revista de Internet, Derecho y Política* (núm. 5).

Piñar Mañas, J. L. (2014). «Transparencia y derecho de acceso a la información pública, algunas reflexiones en torno al derecho de acceso en la Ley 19/2013 de Transparencia, Acceso a la información pública y Buen Gobierno». *Revista Catalana de Dret Públic* (núm. 49).

Puente Escobar, A. (2006). «Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal». A: J. L. Piñar Mañas (dir.). *Protección de datos de carácter personal en Iberoamérica*. València: Agència Espanyola de Protecció de Dades / Tirant lo Blanch.

Rebollo Delgado, L.; Serrano Pérez, M. M. (2008). *Introducción a la protección de datos*. Madrid: Dykinson.

Rubio Torrano, E. (2018). «El Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal». *Revista doctrinal Aranzadi Civil-Mercantil* (núm. 1).

Troncoso Reigada, A. (2012). «Hacia un nuevo marco jurídico europeo de protección de datos personales». *Revista Española de Derecho Europeo* (núm. 43).

Publicacions

Agència dels Drets Fonamentals de la Unió Europea / Consell d'Europa (2018). *Handbook on European data protection law.* Luxemburg.

Agència Espanyola de Protecció de Dades (2015). «Criterio interpretativo: aplicación de los límites al derecho de acceso a la información». Madrid: AEPD.

Agència Espanyola de Protecció de Dades (2016). «Orientaciones y garantías en los procedimientos de anonimización de datos personales». Madrid: AEPD.

Agència Espanyola de Protecció de Dades (2018). «Adaptación al RGPD, Administraciones Públicas». Madrid: AEPD.

Agència Espanyola de Protecció de Dades. (2018). «Guía para el cumplimiento del deber de informar». Madrid: AEPD.

Agència Espanyola de Protecció de Dades (2018). «Los derechos para proteger los datos personales». Madrid: AEPD.

Agència Espanyola de Protecció de Dades (2018). «Protección de datos y administración local». Madrid: AEPD.

Legislació

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). <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>.

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. <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0045&from=ES>.

Llei orgànica 5/1992, de 29 d'octubre, de regulació del tractament automatitzat de les dades de caràcter personal. *Butlletí Oficial de l'Estat,* 31 d'octubre de 1992, núm. 262. <https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189>.

Llei orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal. *Butlletí Oficial de l'Estat,* 14 de desembre de 1999, núm. 298. <https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>.

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. *Butlletí Oficial de l'Estat,* 19 de gener de 2008, núm. 17. <https://www.boe.es/buscar/act.php?id=BOE-A-2008-979>.

Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals. *Butlletí Oficial de l'Estat,* 6 de desembre de 2018, núm. 294. <https://www.boe.es/eli/es/lo/2018/12/05/3>.

Jurisprudència

Sentència del Tribunal Constitucional, núm. 110/1984, de 26 de novembre, relativa a un supòsit fàctic en què es debat una qüestió d'índole tributària. <http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/363>.

Sentència del Tribunal Constitucional, núm. 254/1993, de 20 de juliol. <http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2383>.

Sentència del Tribunal Constitucional, núm. 290/2000, de 30 de novembre. *Butlletí Oficial de l'Estat,* 4 de gener de 2001, núm. 4. El contingut reconeix la competència exclusiva de l'Agència Espanyola de Protecció de Dades per a la gestió i el control de l'obligació d'inscripció dels fitxers de titularitat privada que es reconeixia a la legislació anterior, la LORTAD (1992) i la LOPD (1999). <http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4274>.

Sentència del Tribunal Constitucional, núm. 292/2000, de 30 de novembre. *Butlletí Oficial de l'Estat,* 4 de gener de 2001, núm. 4. El contingut es basa en els pronunciaments derivats del recurs d'inconstitucionalitat presentat pel Defensor del Poble respecte als articles 21.1 i 24.1 i 2 de la LOPD (1999). <http://hj.tribunalconstitucional.es/HJ/cs-CZ/Resolucion/Show/SENTENCIA/2000/292>.

Sentència de la sala contenciosa administrativa de l'Audiència Nacional, 15 de març de 2002, Secció Primera. Fonament jurídic tretzè. <https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/audiencia_nacional/common/pdfs/Sentencia_AN_15_3_2002_y_Sentencia_TS_Recurso_Casacion_25_9_2006.pdf>.

Sentència de la sala contenciosa administrativa del Tribunal Suprem, de 25 de setembre de 2006, Secció Sisena (Recurs de Cassació núm. 3223/2002). Fonament jurídic cinquè. <https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/audiencia_nacional/common/pdfs/Sentencia_AN_15_3_2002_y_Sentencia_TS_Recurso_Casacion_25_9_2006.pdf>.

Sentència del Tribunal de Justícia de les Comunitats Europees (a partir d'ara, «STCE»), de data, 6 de novembre de 2003 (Assumpte C-101/2001), en què s'analitza el supòsit d'una catequista sueca, que, després d'haver fet un curs d'informàtica, publica un seguit de dades personals de diversa índole sobre diversos companys feligresos a la xarxa, sense que els n'hagués advertit prèviament. L'actuació va ser sancionada per incompliment de diversos preceptes establerts a la legislació sueca. <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN>.

Sentència del TJUE, 9 de novembre de 2010 (Cas Volker und Markus Schecke GbR (C-92/09) i Hartmut Eifert (C-93/09) contra Land Hessen). <http://curia.europa.eu/juris/liste.jsf?language=es&num=C-92/09>.

Sentència del Tribunal de Justícia de la Unió Europea (a partir d'ara, «STJUE») de data, 24 de novembre de 2011 (assumptes acumulats C 468/10 i C 469/10), que tenen per objecte les peticions de decisió prejudicial que planteja l'Associació Nacional d'Establiments Financers de Crèdit (ASNEF) (assumpte C#468/10) i la Federació de Comerç Electrònic i Màrqueting Directe (FECEMD) (assumpte C#469/10), relatives a la interpretació de l'article 7, lletra f) de la Directiva 95/46/CE. <http://curia.europa.eu/juris/document/document.jsf?docid=115205&doclang=ES>.