Tema 5. Protecció de dades personals

«[…] en el moment en què tenen de nosaltres adreça, estat civil, edat, ingressos, marca del cotxe, compres, hàbits de beguda i impostos, ja ens han caçat: som una unitat demogràfica d'una persona» (Negroponte, 2003)

L'objectiu principal del tema és oferir un acostament al marc legal de la protecció de dades personals a Europa, amb un interès especial pel que fa a Espanya.

Com a objectius d'aprenentatge, destaquem sintetitzar els elements fonamentals de la protecció de dades i argumentar el text legal aplicable en casos reals.

Advertim en aquest moment que aquests apunts no pretenen en cap moment substituir la consulta de la legislació, sinó simplement servir de suport docent. Cal deixar clar que se simplifica per a poder donar-ne compte en el temps que hi ha reservat en els plans docents, per la qual cosa per a concretar-ne el coneixement de cara a l'execució pràctica, es fa imprescindible acudir al text legal. Perquè els apunts actuals servisquen de full de ruta, quan se cite un dret concret, s'indica quin és l'article de la norma concreta on es pot consultar de manera completa i no resumida.

L'eix que vertebra els apunts és el Reglament Europeu de Protecció de Dades, encara que òbviament no és l'única norma al·ludida.

Introducció

Quan abordem el tema de la protecció de dades personals, hem de tenir en compte que tractem de la protecció d'un dret constitucional fonamental, que ja en 1978 s'incloïa en la Constitució espanyola.

> Article 18 de la Constitució espanyola
>
> 1. Es garanteix el dret a l'honor, a la intimitat personal i familiar i a la imatge pròpia.
>
> 2. El domicili és inviolable. Cap entrada o registre s'hi pot fer sense consentiment del titular o resolució judicial, excepte cas de delicte flagrant.
>
> 3. Es garanteix el secret de les comunicacions i, especialment, de les postals, telegràfiques i telefòniques, excepte resolució judicial.
>
> 4. La llei limitarà l'ús de la informàtica per a garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets.

Hem de ser conscients que es tracta d'un assumpte que genera molta confusió. A més de considerar-lo dret fonamental, hi veiem que s'identifica amb molts altres termes: privacitat,

intimitat, secret, dret fonamental, llei… Hi veiem com les paraules «protecció de dades» ens fan pensar en moltes coses.

Pot ser que la resposta es base en el fet que es tracta d'una mica de tot. Parlem d'un dret fonamental, d'una disciplina jurídica, de llei orgànica… de tot alhora. Encara que per a nosaltres serà, de manera principal, quasi sinònim de «*llei*». De la llei que han d'aplicar i conèixer almenys en les parts fonamentals tots els professionals de la informació que d'alguna manera treballen amb dades de caràcter personal. I, per a ajudar a centrar l'assumpte, descobrim tot seguit com és el text legal per excel·lència d'aquest tema: el Reglament Europeu de Protecció de Dades (Diari Oficial de la Unió Europea, 2016),[1] i fixem-nos en particular en els articles segon i tercer, en els quals es delimita l'àmbit del reglament.

Descobrim que s'aplica al tractament totalment o parcialment automatitzat de dades personals, així com al tractament no automatitzat de dades personals contingudes o destinades a ser incloses en un fitxer, encara que amb una sèrie d'excepcions llarga. Així, hi veiem que no s'aplica en l'exercici d'una activitat no compresa en l'àmbit d'aplicació del Dret de la Unió; quan es tracte del tractament que du a terme una persona física en l'exercici d'activitats exclusivament personals o domèstiques o quan es tracta d'un tractament de les autoritats competents amb finalitats de prevenció, investigació, detecció o enjudiciament d'infraccions penals, o d'execució de sancions penals, inclosa la de protecció davant d'amenaces a la seguretat pública i prevenció.

Hi veiem que s'aplica, el reglament, a les persones físiques, però no es regula el tractament de dades personals relatives a persones jurídiques i en particular a empreses constituïdes com a persones jurídiques, inclòs el nom i la forma de la persona jurídica i les dades de contacte. (considerant 14)

Concretament, l'àmbit del reglament és el tractament de dades personals en el context de les activitats d'un establiment del responsable[2] o de l'encarregat a la Unió, independentment que el tractament tinga lloc a la Unió o no. S'aplica sobre els interessats que estiguen en la Unió per part d'un responsable o encarregat no establit a la Unió, quan les activitats de tractament estiguen relacionades amb l'oferta de béns o serveis, el control del seu comportament, si té lloc a la Unió.

Hi veiem que ja apareixen paraules que necessiten definir-se: per exemple, «el responsable o encarregat del tractament». Més avant, d'ací a unes quantes pàgines, podrem trobar-les en aquest mateix tema.

La protecció de les persones físiques en relació amb el tractament de dades personals és un dret fonamental, com avançàvem, però que, a més, ho confirma el reglament en el considerant primer. I encara més, s'indica expressament que el tractament de dades personals ha d'estar concebut per a servir a la humanitat. Però s'hi afig un matís que ens donarà molt de joc: el dret

[1] Com que aquesta norma s'hi fa servir d'una manera exhaustiva, n'ometrem fins i tot la citació. Així, si parlem d'articles o considerants, ho fem en tot moment en al·lusió al Reglament Europeu de Protecció de Dades, si no s'indica una altra cosa. Ometem, excepte citacions textuals on es referencie així, les sigles anglosaxones GDPR que hi al·ludeixen.

[2] En breu, veurem les definicions de les figures principals: responsable del tractament, encarregat del tractament i delegat de dades.

a la protecció de les dades personals no és un dret absolut sinó que s'ha de considerar en relació amb la funció que té en la societat i mantenir l'equilibri amb altres drets fonamentals, conformement al principi de proporcionalitat (considerant 4). Això ja ho anticipava (Davara Rodríguez, 1998) una dècada abans del text literal del reglament.

El reglament no s'aplica a qüestions de protecció dels drets i les llibertats fonamentals o la lliure circulació de dades personals relacionades amb activitats excloses de l'àmbit del Dret de la Unió, com les activitats relatives a la seguretat nacional. Tampoc s'aplica al tractament de dades de caràcter personal pels Estats membres en l'exercici de les activitats relacionades amb la política exterior i de seguretat comuna de la Unió (considerant 16). De la mateixa manera, tampoc s'aplica al tractament de dades de caràcter personal per una persona física en el curs d'una activitat exclusivament personal o domèstica (com la correspondència, una agenda personal o l'activitat en les xarxes socials). Sí que s'aplica als responsables o encarregats del tractament que proporcionen els mitjans per a tractar dades personals relacionades amb tals activitats personals o domèstiques (considerant 18).

Hem de tenir clar que el dret no és un conjunt de disciplines autoexcloents. Sovint se solapen entre si, com en aquest cas, per exemple, ocorre amb les normes que regeixen la llibertat d'expressió i informació, inclosa l'expressió periodística, acadèmica, artística o literària, i el dret a la protecció de les dades personals. Pel que fa al cas, el tractament de dades personals està subjecte a excepcions o exempcions si així es requereix per a conciliar el dret a la protecció de les dades personals amb altres drets (considerant 153).

El problema que sorgeix en regular qualsevol dret fonamental és que s'ha de fer sense posar en perill altres drets fonamentals. No obstant això, el que dos drets no entren en col·lisió és pràcticament utòpic (De Miguel Molina; Oltra Gutiérrez. *Deontología y aspectos legales de la Informática: cuestiones jurídicas, técnicas y éticas básicas*, 2007). En la protecció de dades, normalment s'entra en col·lisió amb altres dos drets fonamentals:

- el dret a la informació
- la llibertat d'expressió

A més, la col·lisió amb les normes de transparència és evident. Què s'hi ha de fer llavors? Els tribunals apliquen en aquest cas el principi de proporcionalitat, ja que s'ha de veure en cada cas concret quin dret preval. El dret a la informació no és un dret absolut, com tampoc ho és la llibertat d'expressió, i normalment els jutges i magistrats sempre es bolcaran més cap a la intimitat de l'individu que cap als altres drets. Una altra cosa és que hi haja raons d'interès general que aconsellen una altra mesura. Sense pretendre generalitzar, la veritat és que tant el Tribunal Constitucional com el Suprem resolen normalment que el dret a la intimitat preval davant del dret a la informació.

Tractament contra llibertat d'expressió
Quin ha de prevaldre? No hi ha una recepta única. El reglament ens diu que s'han de conciliar tots dos, generant exempcions o excepcions. (article 85)

La ràpida evolució tecnològica i la globalització han plantejat reptes nous per a la protecció de les dades personals des de la normativa anterior. S'ha incrementat la magnitud de l'arreplega i

de l'intercanvi de dades personals, les TIC han facilitat que empreses privades i autoritats públiques utilitzen dades personals en una escala sense precedents a l'hora de dur a terme les seues activitats. Dades que ben sovint ixen directament dels usuaris en una difusió voluntària (xarxes socials, per exemple). No fa falta que recordem que en la nostra societat les dades personals són potencialment generadores del millor i del pitjor: mentre veiem com la intel·ligència artificial fonamentada en grans bases de dades mèdiques comença a aplicar-se en plenitud a la medicina, en paral·lel ens assabentem de com a la Xina s'és capaç d'identificar dues-centes persones per minut, estudiar-ne el comportament passat, present i predictiblement futur i atorgar així carnets de bons ciutadans. En aquest món en el qual la intimitat pareix que s'haja girat al revés com un calcetí i que es nodreix de «m'agrada» i *retweets*, és important generar confiança que permeta l'economia digital desenvolupar-se en tot el mercat interior europeu. Les persones físiques han de tindre el control de les dades personals pròpies. S'ha de reforçar la seguretat jurídica i pràctica per a les persones físiques, els operadors econòmics i les autoritats públiques (considerants 6 i 7). A la recerca d'aquesta seguretat, i dels drets dels ciutadans, s'han de minimitzar les diferències en les normes dels països de la Unió, perquè poden constituir un obstacle a l'exercici de les activitats econòmiques a escala de la Unió (considerant 9).

Un element de molt d'interès apareix quan el reglament es destapa amb una indicació que ens afecta de manera important com a tecnòlegs: es diu expressament que la protecció de les persones físiques ha de ser tecnològicament neutra i no ha de dependre de les tècniques utilitzades. Això implica que en matèria de selecció d'elements de programari i maquinari hem de mantenir «posicions agnòstiques», que servisquen a la finalitat amb independència del mitjà.

No s'ha d'oblidar tampoc una cosa que ja heretem d'abans, de normes anteriors, com ara la Llei orgànica de protecció de dades de 1999 (BOE, 1999): la protecció de les persones físiques s'ha d'aplicar al tractament automatitzat de dades personals, així com al tractament manual, quan les dades personals figuren en un fitxer o estiguen destinades a incloure-les-hi.

Això és: una carpeta de gomes amb fitxes de clients… és un fitxer que s'ha de protegir.

Però, a pesar d'això, hi ha una xicoteta indicació que ens pot evitar molt de treball tècnic, que per la importància que té no hem d'oblidar: els fitxers o conjunts de fitxers, així com les portades, que no estiguen estructurats segons criteris específics, no han d'entrar en l'àmbit d'aplicació del present reglament. (considerant 15)

D'altra banda, no podem deixar de subratllar que no és, ni de bon tros, l'única legislació que s'ha de tenir en compte a l'hora de tractar dades. Pel que fa al cas, és interessant consultar el text de García Mirete (2014). Per exemple, quan parlem d'ús de dades en comunicacions electròniques, hem de fer referència a la LSSI (BOE, 2002). No hem d'oblidar tampoc que les lleis les interpreten els jutges i ben sovint hem de prestar una atenció especial a les interpretacions que en fan.[3]

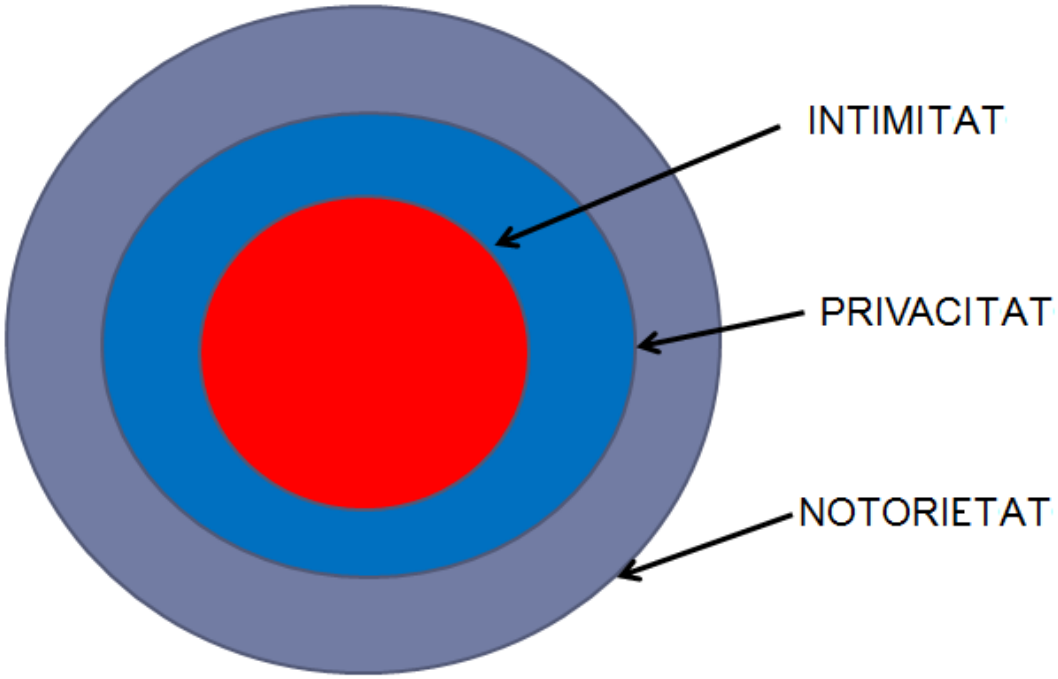
[3] D'exemples, n'hi ha molts. Citem-ne dos, per no fer-ho molt llarg.
La STC 202/1999, 8 de novembre. Recurs d'empara contra les sentències de la sala social del Tribunal Superior de Justícia de Catalunya i del jutjat social número 2 de Barcelona que deneguen la cancel·lació de les dades mèdiques del recurrent les quals es trobaven en un fitxer informàtic sobre «absentisme amb baixa mèdica» de l'entitat creditícia en la qual treballava. Es tracta de: vulneració de dret a la intimitat, negativa a la cancel·lació de dades, fallida de la garantia de la confidencialitat de les dades i inexistència de responsable de fitxer. S'atorga l'empara.

Per a tancar aquest apartat d'introducció, intentarem eliminar unes quantes confusions típiques. La primera és la que sorgeix quan es confonen paraules com ara *dades*, *informació* i *informàtica*. Una dada és difícil que per ella només puga tenir incidència greu en l'anomenada privacitat (Davara Rodríguez, 1998), mentre la dada no resolga una consulta determinada, no done resposta a una pregunta o solució a un problema, pot ser un antecedent, però poca cosa més. La informació és la paret que construïm amb dades, i això ja és un suport ferm. Si sotmetem la informació a tractament (tractament que sol ser informàtic, per la complexitat que té fer manualment accions amb grans quantitats de dades), ja tenim un resultat útil per a una finalitat determinada. I potencialment perillós, segons siga la finalitat. Amb la informàtica s'ofereixen múltiples possibilitats d'emmagatzematge i tractament de la informació, i de recuperació, de formes tan variades i invisibles per al ciutadà que pot arribar a produir verdadera pressió i control social. L'encreuament de dades entre bases de dades, amb el tractament automàtic implícit provoca a vegades la pèrdua de control del titular de les dades, que no és ni més ni menys que la persona a qui les dades descriuen.

Però encara hi ha un altre punt de confusió: totes les dades personals són iguals? Tenen la mateixa importància? Que patim una malaltia degenerativa i es faça públic a les companyies asseguradores té el mateix valor que la dada del nostre número de telèfon o el nom del nostre pare? I si la dada l'hem revelada en un blog, o si prové d'una llista pública? Tot i que aprofundirem en l'assumpte més avant, val la pena fer servir un gràfic ara per a establir, a manera de capes, la major o menor incidència en la nostra vida dels diferents tipus de dades.

Un darrer exemple. Observeu que intencionalment he triat sentències antigues, anteriors a la mateixa LOPD, perquè se'n puguen comparar els efectes amb les normes que hui ens regeixen. Sentència del TSJ d'Andalusia de 6 d'octubre de 1995.

Els ajuntaments estan exclosos de l'obligació de facilitar les dades que consten en el padró a l'efecte d'embargaments i altres diligències executòries, de manera que han de subministrar dades als serveis estadístics estatals únicament als efectes d'elaborar-ne estadístiques.



Il·lustració 1. D'allò íntim a allò notori. Elaboració pròpia

Hem vist de manera molt general què és això de la protecció de dades, què protegeix. I pareix que és una cosa nova, que sorgeix amb les TIC. Però en realitat sempre, d'alguna manera, ha estat ací. Ho veurem.

Una mica d'història

A l'antiga Grècia no hi havia res semblant a la protecció de dades. És a Roma quan apareix el dret de propietat del jo. Es parla d'un home exterior i un altre d'interior.

El temps passa i en l'edat mitjana apareixen sant Agustí parlant de l'home com a portador de valors i sant Tomàs considerant la intimitat com un bé sagrat. Allò privat existeix, però es resumeix i recau sobre el *pater familias*. Continua avançant la història i en l'edat moderna, amb «la raó» i els seus filòsofs, hi ha una nova volta de rosca. Locke, i el seu concepte de la «llibertat negativa» reconeixen a l'individu una esfera íntima. Rousseau hi afig la intimitat des de l'àmbit de la persona.

Hui en dia, sabem que les dades són propietat del titular, del ciutadà. La informació assacia les ànsies de poder de molts, perquè poder és informació. La intimitat ara puja de nivell, no només és ocultació, reserva, sinó la capacitat de decidir en l'esfera íntima.

Veiem com la privacitat, la intimitat de les persones, és una cosa que sempre ens ha preocupat als éssers humans. Inclús a les cases romanes on vivia la no-elit, on s'amuntonaven les famílies, les persones cercaven els seus llocs per a la intimitat, els seus secrets particulars que no desitjaven que es feren públics.

Però, llavors el que preocupava era el rumor. Hui, és la xarxa de xarxes. Hi ha un matís. La informàtica ha suposat una eina important per a tot, bé i mal. Per a trencar aquesta intimitat també. És lògic que cresqueren les normes sobre el tema.

A Espanya, per fer una vista ràpida a la nostra història del dret, podríem viatjar en el passat fins a la llei de l'11 de gener de 1541 en la qual l'emperador Carles I dota d'inviolabilitat les Cartes. Cosa que ja s'estén en un moment tan tardà com la Constitució de 1869 a la inviolabilitat de domicili i, per primera vegada, secret de la correspondència i efectes personals.

En el segle XX, l'única referència prèvia a la nostra constitució actual la trobem en el Fuero de los Españoles del 17 de juliol de 1945. En el títol preliminar apareix un principi fonamental: el respecte a la dignitat i llibertat humanes. Però arribem al 78, i després de la Constitució, apareixen unes quantes lleis, que marquen el camí:

- Llei Orgànica 1/1982, de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la imatge pròpia
- 16/1985 de patrimoni històric espanyol
- 13/1986 de foment i coordinació general de la investigació científica i tècnica
- Altres: 12/1989 reguladora de la funció estadística pública

Per descomptat, apareix la LORTAD en el 92, llei precedent i quasi mare de la nostra LOPD actual, del 99, i sorgeixen diverses lleis que en matisen uns quants aspectes. Per exemple:

- 34/2002 LSSI
- 56/2007 de mesures d'impuls de la societat de la informació
- 25/2007 de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions (lluita contra el terrorisme i el crim organitzat)
- 9/2014 nova llei de telecomunicacions

Però per a definir concretament el nostre marc, deixem clar el que és essencial.

Partint de la pedra basal que és l'article 18 de la Constitució: 4. La llei limitarà l'ús de la informàtica per a garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets.

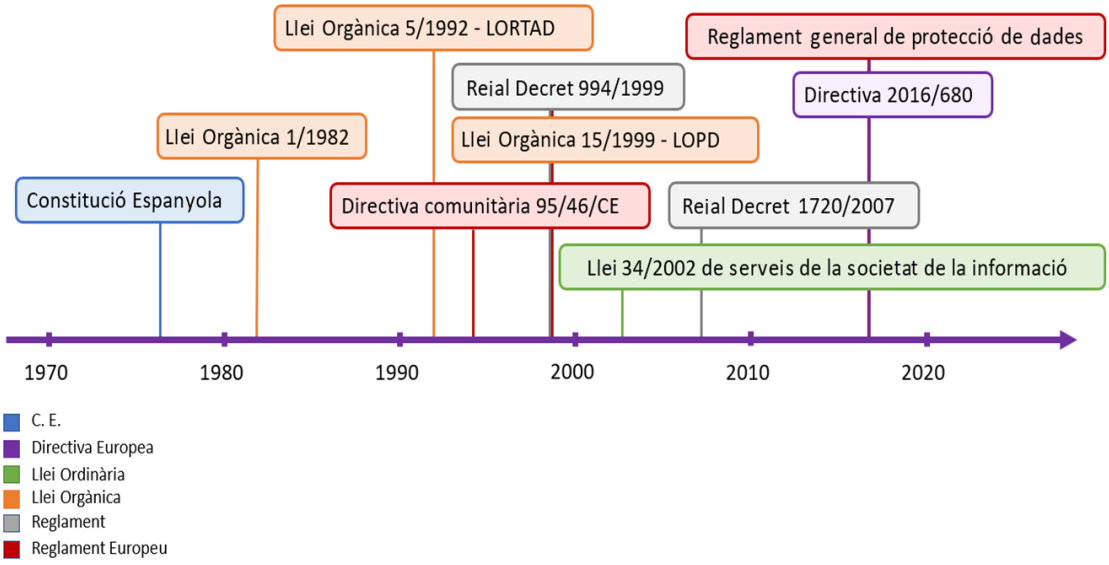
Va aparèixer en el seu moment, condicionada pel protocol de Schengen, «Espai de Llibertat, Seguretat i Justícia») (Goizueta Vértiz, González Murua, Pariente, 2013) la nostra extinta LORTAD, Llei orgànica 5/1992, de 29 d'octubre.

Llei que es va modificar mitjançant el Reial decret 1332/1994, de 20 de juny, pel qual es desenvolupen determinats aspectes de la LORTAD, i es va reglamentar amb el Reial decret 994/1999, d'11 de juny, reglament de mesures de seguretat dels fitxers automatitzats que continguen dades de caràcter personal.

Una directiva comunitària (95/46/CE de 24/octubre/95) exigia l'extensió a fitxers manuals. Això va provocar el naixement de la LOPD, Llei orgànica 15/1999, de 13 de desembre, i posteriorment del Reial decret 1720/2007, de 21 de desembre, reglament de desenvolupament de la Llei orgànica 15/1999.

Actualment es troba com a avantprojecte una nova LOPD, i resta suspesa la llei del 99 en tot el que contradiga el Reglament europeu de protecció de dades.

Podem veure'n un fil temporal en la imatge següent:



Il·lustració 2. Legislació sobre protecció de dades (Gámiz Mejías & Oltra Gutiérrez (director), 2018). Adaptat

I què ocorria al «món»?

En els ordenaments d'àmbit anglosaxó se n'ha anomenat «*privacy*», ací adaptat com a «privacitat» (Davara Rodríguez, 1998). No és exactament el mateix, però atesa la segona accepció que té ('Àmbit de la vida privada que es té dret a protegir de qualsevol intromissió'), podem establir per al nostre treball una certa identitat.

Quan es data l'origen de la privacitat en el món anglosaxó?

Pareix que hi ha una coincidència generalitzada a indicar que van ser Samuel D. Warren i Louis D. Brandeis (Warren i Brandeis, 1890) qui en «Dret a la privacitat» van fonamentar en el principi d'inviolabilitat a la persona els límits jurídics a la intromissió en la vida de les persones. Garriga (Garriga Domínguez, 2010) indica que poc després d'aquesta aplicació comença a fer-ne ús un tribunal de Nova York emprant l'expressió encunyada (*the right to privacy*), que a partir de llavors es multiplicaria en resolucions judicials (encara que també s'usara amb el curiós nom de «dret a ser deixat en pau»).

Als Estats Units (seguim Garriga en aquest punt), William Prosser publica en 1960 un assaig usant les línies mestres de Warren i Brandeis, en què assenta les possibles violacions del dret a la intimitat en la societat moderna. L'any següent, 1961, travessa l'oceà i se succeeixen al Regne Unit diversos projectes de llei per a la creació d'un dret autònom a la intimitat. Apareixen els estudis de Frosini, Alan F. Westin i, al nostre país, de Pérez Luño, que divulguen al llarg dels dos continents aquestes idees (Garriga Domínguez, 2010). Convé precisar que mentre a Europa es parla de protecció de dades, als Estats Units es parla de privacitat sense abordar pròpiament quin és l'objecte de protecció i quins mitjans tècnics poden contribuir a protegir les dades.

Sense cenyir-nos a l'àmbit anglosaxó, ja en 1948 el dret a la intimitat és inclòs en l'article 12 de la Declaració dels Drets Humans, i molt poc després, es reflecteix en l'article 8 del Conveni de Roma, en 1950.

Al maig del 67, en la Conferència de Juristes Nòrdics, s'aconsella la protecció de la vida privada mitjançant instruments específics i més adequats a les noves formes d'ingerència. Naix a Europa l'esperit de la protecció de dades. Això dona pas a la creació d'una comissió consultiva del Consell d'Europa, per a estudiar les tecnologies de la informació i la influència que tenen sobre els drets de la persona, que al seu torn emet la Resolució 68/509/CE de l'Assemblea del Consell d'Europa, sobre «els drets humans i els nous assoliments científics i tècnics».

En un àmbit superior, a l'ONU, mentrestant, el 19 de desembre de 1968 apareix la Resolució 2450 (XXIII), en la qual s'estableix la necessitat de fixar límits a les aplicacions de l'electrònica, que culmina en 1983 amb un informe relatiu als principis respecte a la utilització dels fitxers informatitzats de caràcter personal.

El món continua girant i en 1970, el 23 gener, sorgeix la resolució 428 de l'Assemblea Consultiva del Consell d'Europa: «intimitat com un objecte de protecció obligada enfront de la intromissió de la tecnologia de la informació». Això dona pas al fet que en 1973 sorgisca la resolució (73) 22, de 26 de setembre: «protecció de la vida privada de les persones físiques enfront del sector privat» i en 1974 (29) el mateix, sobre el sector públic. Es poden veure unes reflexions ben interessants sobre les resolucions (73) 22 i (74) 29 en el text referenciat en bibliografia de Davara (Davara Rodríguez, 1998). És el moment en què comencen a inspirar-se uns quants estats, com ara l'alemany, per a aprovar lleis, com l'alemanya Llei de Hesse, de 1970, que vol protegir el dret de la personalitat restringint la utilització de dades personals que puguen afectar els ciutadans per part de l'administració. Molt ràpidament, en 1974, es promulga la primera *Privacy Act* dels Estats Units d'Amèrica del Nord. És en aquesta etapa quan s'introdueix la idea de la protecció efectiva a les persones enfront de l'ús informatitzat de les dades. Una tercera etapa la marca la internacionalització de la protecció del dret fonamental a l'autodeterminació informativa (Garriga Domínguez, 2010).

El 1980, el 28 de setembre, el Consell de Ministres del Consell d'Europa dona llum al conveni per a la protecció de les persones respecte al tractament automatitzat de dades de caràcter personal. És el Conveni 108 per a la protecció de les persones respecte al tractament automatitzat de dades de caràcter personal del Consell d'Europa (publicat en 1981). Ací s'intenta harmonitzar el principi de lliure circulació internacional de dades personals amb la defensa de drets i llibertats de les persones, però a més es complementen els principis relatius a la qualitat de les dades.

El mateix any 1980 apareix la recomanació de l'OCDE sobre circulació internacional de dades personals i la protecció de la intimitat, centrada en persones físiques i on sorgeixen els que més tard serien considerats els principis bàsics de la protecció de dades.

No hem esmentat sentències interessants, com la que desenvolupa el «principi de consentiment», o el «dret d'autodeterminació», procedents del Tribunal Constitucional alemany, de 1983, que van inspirar la llei alemanya de 1990 i que es va expandir per la resta del continent.

L'evolució que implica passar de la privacitat com a dret d'exclusió dels altres de l'àmbit privat a una configuració com a llibertat negativa enfront de la informació abusiva dels nostres dies ha suposat un pas de gegant: hui es concep com una llibertat positiva, la llibertat d'exercir un dret de control sobre les dades referides a la persona que ja han eixit de l'esfera de la intimitat per a convertir-se en element d'un arxiu electrònic privat o públic.

Ja l'any 1978 James Martin explicava com en la societat de les telecomunicacions els éssers humans podem sentir-nos com els ossos polars que porten incorporat un radiotransmissor en miniatura que permet enregistrar i enviar a un satèl·lit els passos que fan. Els grans bancs de dades de les administracions públiques i grans corporacions que apareixen en aquestes dates van fer possible una vigilància real de la vida quotidiana, permeteren imputar a un individu certes pautes de comportament, comunes a grups censats i que distingim de la resta de la població global (Garriga Domínguez, 2010).

Això és el que Frosini (1982) ha denominat la llibertat informàtica: el dret a autotutela de la identitat informàtica pròpia, això és, la que resulta de l'arreplega i la confrontació de les dades personals inserides en un sistema informàtic. El respecte a la intimitat s'estén hui a una esfera àmplia de la vida privada. No només es tracta d'informes íntims sinó també de comportaments personals, elements diferents de la personalitat, opinions religioses i polítiques… dades anomenades sensibles per a distingir-les de les que hi ha a la disposició del públic.

Es pot observar que l'interès jurídic, centrat positivament, primitivament, sobre el problema de la tutela de la intimitat personal, ha variat la significació cap a l'enteniment com a un dret subjectiu, desplaçament provocat per la profusió d'ús d'arxius magnètics i bancs de dades personals.

Ja es tracta de llibertat de controlar l'ús de les dades personals pròpies inserides en un programa informàtic: és l'*habeas data*, corresponent a l'*habeas corpus* del respecte degut a la integritat i llibertat de la persona i per tant obri el dret d'accés dels bancs de dades; el dret de control de la seua activitat: el dret de rectificació; el dret de secret per dades sensibles; el dret a donar autorització per a fer-ne difusió… és, en si, una darrera etapa, en la qual ens preocupa la incidència d'Internet i els avanços científics, com el desxiframent del mapa genètic.

Però tornem al principi. Ens preguntàvem: és un dret fonamental, una disciplina jurídica?

És un dret fonamental? El Tribunal Constitucional (sentència TC 292/2000) diu que sí.

Com a disciplina jurídica busca protegir la intimitat i altres drets fonamentals de les persones físiques davant del risc que suposa la recopilació i l'ús indiscriminat de les dades personals, abasta tot tipus de tractament (independentment que es faça de manera manual o informatitzada) i marca la necessitat de desenvolupar normes que, limitant l'ús de les dades personals, garantisquen l'honor i la intimitat personal i familiar dels ciutadans.

Principis de la llei

Convé abans d'entrar en definicions que centrem que és el que s'espera del tractament de dades. Entra en joc una paraula, *qualitat*, que pot portar-nos imatges ben diferents. Per a un

espectador aliè a la llei, pot ser que la primera impressió de la qualitat de les dades siga que han de ser com més completes i exhaustives millor. Però estaria molt equivocat.

Per qualitat de les dades s'ha considerat tradicionalment el compliment d'una sèrie de característiques:

- Pertinència: les dades personals han d'estar relacionades amb la finalitat perseguida, per la qual cosa han de ser adequades i no excessives.
- Finalitat: només es poden arreplegar i tractar les dades que siguen adequades amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'hagen obtingut.
- Veracitat i exactitud: les dades han de ser exactes i actualitzades de manera que responguen amb veracitat a la situació de l'interessat: han de ser dades actualitzades i també ser veraces.
- Lleialtat: les dades personals les ha d'arreplegar sense enganys o falsedats qui les sol·licita.
- Seguretat: han d'adoptar-se les mesures necessàries per a garantir la seguretat de les dades personals evitant alteració, pèrdua, tractament o accés no autoritzats.

Si ens n'anem a l'article 5 del reglament, trobem els principis que estableix la llei, que veurem que és un eco d'això que anticipàvem. Així, en l'article dit trobem les exigències següents:

- Licitud, lleialtat i transparència.
- Limitació de la finalitat: arreplegades amb finalitats determinades, explícites i legítimes, i no seran tractades ulteriorment de manera incompatible amb aquestes finalitats.
- Minimització de dades: adequades, pertinents i limitades al que siga necessari en relació amb les finalitats per a les quals són tractades.
- Exactitud: exactes i actualitzades.
- Integritat i confidencialitat: es garanteix una seguretat adequada de les dades personals.

Hem d'afegir-hi, i això és important i un canvi d'enfocament fonamental, que el responsable del tractament serà responsable del compliment i capaç de demostrar-ho («responsabilitat proactiva»).

Ampliem el terme que pot ser més confús, la «licitud del tractament» (vegeu l'article 6). El tractament només serà lícit si es compleix almenys una de les condicions següents: o l'interessat va donar el consentiment per al tractament de les seues dades personals per a una o diverses finalitats específiques, o el tractament és necessari per a l'execució d'un contracte en el qual l'interessat és part o per a l'aplicació a petició d'aquest de mesures precontractuals; o és necessari per al compliment d'una obligació legal aplicable al responsable del tractament; o és necessari per a protegir interessos vitals de l'interessat o d'una altra persona física; o és necessari per al compliment d'una missió feta en interès públic o en l'exercici de poders públics conferits al responsable del tractament; o és necessari per a la satisfacció d'interessos legítims perseguits pel responsable del tractament o per un tercer, sempre que sobre aquests interessos

no prevalguen els interessos o els drets i llibertats fonamentals de l'interessat que requerisquen la protecció de dades personals, en particular quan l'interessat és un xiquet.

> Un interès legítim és la necessitat de saber si un sistema d'informació és capaç de resistir, en un nivell determinat de confiança, esdeveniments accidentals o accions il·lícites o malintencionades que comprometen la disponibilitat, autenticitat, integritat i confidencialitat de les dades personals conservades o transmeses, i la seguretat dels serveis connexos que ofereixen aquests sistemes i xarxes, o accessibles a través dels dits sistemes i xarxes, per part d'autoritats públiques, 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 tractar d'impedir l'accés no autoritzat a les xarxes de comunicacions electròniques i la distribució malintencionada de codis, i frenar atacs de «denegació de servei» i danys als sistemes informàtics i de comunicacions electròniques. (considerant 49)

Quan el tractament per a una altra finalitat diferent d'aquella per a la qual es van arreplegar les dades personals no estiga basat en el consentiment de l'interessat o en el Dret de la Unió o dels Estats membres, el responsable del tractament ha de tenir en compte, entre altres, qualsevol relació entre les finalitats per a les quals s'arrepleguen les dades personals i les finalitats del tractament ulterior previst; el context en què s'hagen arreplegat les dades personals, en particular pel que fa a la relació entre els interessats i el responsable del tractament; la naturalesa de les dades personals, sobretot si pertanyen a categories especials de dades personals; les possibles conseqüències per als interessats del tractament ulterior previst, i l'existència de garanties adequades, que poden incloure l'encriptació o la pseudonimització.[4]

Definicions

L'article 4 del reglament europeu ens dona una sèrie de definicions que seran les rajoles amb les quals construïm les idees d'aquest tema. Directament d'allí, tan sols introduint alguna nota aclaridora, són les que hi ha ací. Cal fer-hi una apreciació: les definicions pareix que es mostren com les cireres d'una cistella, de les quals en agafar-ne una te n'endús darrere unes quantes més. Això podem veure-ho clarament en la primera, «dades personals», en què per a definir el terme alhora que es defineix què és una persona física identificable i, per enumeració, un identificador. Així, es parla de:

[4] Entenem pseudonimització com el procediment mitjançant el qual es reemplacen camps d'informació personal dins d'un registre de dades per un o més identificadors artificials (pseudònims) aconseguint així que cada registre siga menys identificable, però igualment apte per a fer-ne el processament. El reglament l'ofereix com a alternativa a l'anonimització (considerem que és un procés irreversible, i les dades personals deixen de ser identificables, amb l'avantatge d'evitar el dret a l'oblit amb un esborrament complet, amb la qual cosa podem continuar generant mètriques clau per al negoci). Una possible pseudonimització és l'encriptació, que no es pot revertir sense la clau de desencriptació). En aquest cas, aquesta clau s'ha de guardar separadament de les dades pseudonimitzades. Cal subratllar que les dades pseudonimitzades continuen sent dades personals (considerant 26), emparades pel Reglament General de Protecció de Dades. La definició oficial del terme, procedent del reglament, apareix en l'apartat «Definicions» d'aquest mateix tema.

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 puga determinar, directament o indirectament, en particular mitjançant un identificador, com ara un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona.

Hem de tenir en compte que una dada, en si, no és ni bona ni roín, ni assenyala ni deixa d'assenyalar. És la unió entre dades el que ens preocupa, encara que a vegades també ho fan dades soltes. Un exemple: òbviament no és el mateix dir 65, que «Hermògenes Finisterre Brodovín té 65 anys». Un exemple més ampli en la taula següent:

Dades aïllades no afectades	Dades afectades
1979	Alberto Martínez Pujol
46071	http:\\www.pepemaiquez.net
95%	158.153.205.26
Barcelona	C\ Ànec Coix, 23, pta. 18
Groc	jacinto.quincoces@gmail.com

Taula 1. Dades aïllades afectades i no afectades. Elaboració pròpia

Tractament: qualsevol operació o conjunt d'operacions fetes sobre dades personals o conjunts de dades personals, ja siga per procediments automatitzats o no, com arreplega, registre, organització, estructuració, 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.

Convé en aquest punt recordar la divisió per temps, per moments, del tractament, que suggeria Davara Rodríguez (1998):

1. Arreplega
2. Tractament en si (encreuament, relació…)
3. Utilització i si escau comunicació (cessió)

Limitació del tractament: el marcatge de les dades de caràcter personal conservades amb la finalitat de limitar-ne el tractament en el futur.

Un exemple extrem de limitació del tractament poden ser les llistes Robinson.

Són llistes que elabora amb totes les garanties legals la Federación Española de Comercio Electrónico y Marketing Directo, de manera que elabora unes llistes de possibles clients en funció de les preferències a l'hora de rebre publicitat o un altre tipus de promocions. Les empreses adherides a la federació hi tenen accés i les persones inscrites la possibilitat de sol·licitar la cancel·lació i supressió de les seues dades en tot moment.

És una bona possibilitat, igual que el cens promocional però més personalitzat, de fer enviaments publicitaris de manera legal, perquè en internet proliferen diverses bases de dades totalment il·legals que poden plantejar problemes a les organitzacions poc cauteloses.

Elaboració de perfils: tota forma de tractament automatitzat de dades personals consistent a utilitzar dades personals per a avaluar determinats aspectes personals d'una persona física, en particular per a analitzar o predir aspectes relatius al rendiment professional, situació econòmica, salut, preferències personals, interessos, fiabilitat, comportament, ubicació o moviments d'aquesta persona física.

Pseudonimització: el tractament de dades personals de manera que ja no es puguen atribuir a un interessat sense utilitzar informació addicional, sempre que la informació addicional figure separadament i estiga subjecta a mesures tècniques i organitzatives destinades a garantir que les dades personals no s'atribuïsquen a una persona física identificada o identificable.

Fitxer: tot conjunt estructurat de dades personals, accessibles conformement a criteris determinats, ja siga centralitzat, descentralitzat o repartit de manera funcional o geogràfica.

Responsable del tractament o «responsable»: la persona física o jurídica, autoritat pública, servei o altre organisme que, sol o junt amb altres, determine 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 a nomenar-lo podrà establir-los el Dret de la Unió o dels Estats membres.

Encarregat del tractament o «encarregat»: la persona física o jurídica, autoritat pública, servei o altre organisme que tracte dades personals per compte del responsable del tractament.

Destinatari: la persona física o jurídica, autoritat pública, servei o altre organisme al qual es comuniquen dades personals, es tracte o no d'un tercer. No obstant això, no es consideren destinataris les autoritats públiques que puguen rebre dades personals en el marc d'una investigació concreta de conformitat amb el Dret de la Unió o dels Estats membres; el tractament d'aquestes dades per part d'aquestes autoritats públiques ha de ser conforme a les normes en matèria de protecció de dades aplicables a les finalitats del tractament.

Tercer: persona física o jurídica, autoritat pública, servei o organisme diferent de l'interessat, del responsable del tractament, de l'encarregat del tractament i de les persones autoritzades per a tractar les dades personals sota l'autoritat directa del responsable o de l'encarregat.

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

Violació de la seguretat de les dades personals: tota violació de la seguretat que ocasione la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o l'accés no autoritzats a les dites dades.

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

Què són les dades genètiques? Es tracta de les dades personals relacionades amb característiques genètiques, heretades o adquirides, d'una persona física, provinents de l'anàlisi d'una mostra biològica de la persona física en qüestió, en particular a través d'una anàlisi cromosòmica, una anàlisi de l'àcid desoxiribonucleic (ADN) o de l'àcid ribonucleic (ARN), o de l'anàlisi de qualsevol altre element que permeta obtenir informació equivalent. (considerant 34)

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 permeten o confirmen la identificació única d'aquesta persona, com ara imatges facials o dades dactiloscòpiques.

Dades relatives a la salut: dades personals relatives a la salut física o mental d'una persona física, inclosa la prestació de serveis d'atenció sanitària, que revelen informació sobre l'estat de salut que té.

Sobre les dades relatives a la salut, han d'incloure totes les dades relatives a l'estat de salut de l'interessat que donen informació sobre el seu estat de salut física o mental passat, present o futur. S'inclou la informació sobre la persona física arreplegada en ocasió de la inscripció a l'efecte d'assistència sanitària, o en ocasió de la prestació de tal assistència; tot número, símbol o dada assignada a una persona física que la identifique de manera unívoca a efectes sanitaris; la informació obtinguda de proves o exàmens d'una part del cos o d'una substància corporal, inclosa la procedent de dades genètiques i mostres biològiques, i qualsevol informació relativa, a títol d'exemple, a una malaltia, una discapacitat, el risc de patir malalties, l'historial mèdic, el tractament clínic o l'estat fisiològic o biomèdic de l'interessat, independentment de la font, per exemple un metge o un altre professional sanitari, un hospital, un dispositiu mèdic o una prova diagnòstica in vitro. (considerant 35)

És d'interès la Directiva 2011/24/UE del Parlament Europeu i del Consell, de 9 de març de 2011, relativa a l'aplicació dels drets dels pacients en l'assistència sanitària transfronterera (DO L 88 de 4.4.2011, p. 45).

Establiment principal: pel que fa a un responsable del tractament amb establiments en més d'un Estat membre, el lloc de la seua administració central a la Unió, llevat que les decisions sobre les finalitats i els mitjans del tractament es prenguen en un altre establiment del responsable a la Unió i aquest últim establiment tinga el poder de fer aplicar aquestes decisions, en aquest cas l'establiment que haja adoptat aquestes decisions es considera establiment principal. Pel que fa a un encarregat del tractament amb establiments en més d'un Estat membre, el lloc de la seua administració central a la Unió o, si no en tinguera, l'establiment de l'encarregat a la Unió en el qual es duen a terme les principals activitats de tractament en el context de les activitats d'un establiment de l'encarregat en la mesura en què l'encarregat estiga subjecte a obligacions específiques conformement al present reglament.

Representant: persona física o jurídica establida a la Unió que, designada per escrit pel responsable o l'encarregat del tractament conformement a l'article 27 del reglament,

represente el responsable o l'encarregat pel que fa a les obligacions respectives en virtut del present reglament.

Empresa: persona física o jurídica dedicada a una activitat econòmica, independentment de la forma jurídica, incloses les societats o associacions que exercisquen regularment una activitat econòmica.

Grup empresarial: grup constituït per una empresa que exerceix el control i les seues empreses controlades.

Normes corporatives vinculants: les polítiques de protecció de dades personals assumides per un responsable o encarregat del tractament establit al 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.

Autoritat de control: l'autoritat pública independent que estableix un Estat membre conformement al que es disposa en l'article 51 del reglament.

Autoritat de control interessada: l'autoritat de control a la qual afecta el tractament de dades personals pel fet que el responsable o l'encarregat del tractament està establit en el territori de l'Estat membre d'aquesta autoritat de control; o els interessats que resideixen en l'Estat membre d'aquesta autoritat de control es veuen substancialment afectats o és probable que es vegen substancialment afectats pel tractament, o s'ha presentat una reclamació davant d'aquesta autoritat de control.

Tractament transfronterer: el tractament de dades personals fet en el context de les activitats d'establiments en més d'un Estat membre d'un responsable o un encarregat del tractament a la Unió, si el responsable o l'encarregat està establit en més d'un Estat membre; o el tractament de dades personals fet en el context de les activitats d'un únic establiment d'un responsable o un encarregat del tractament a la Unió, però que afecta substancialment o és probable que afecte substancialment interessats en més d'un Estat membre.

Objecció pertinent i motivada: l'objecció a una proposta de decisió sobre l'existència o no d'infracció del present reglament, o sobre la conformitat amb el present reglament d'accions previstes en relació amb el responsable o l'encarregat del tractament, que demostre clarament la importància dels riscos que comporta el projecte de decisió per als drets i llibertats fonamentals dels interessats i, si escau, per a la lliure circulació de dades personals dins de la Unió.

Servei de la societat de la informació: tot servei conforme a la definició de l'article 1, apartat 1, lletra b), de la Directiva (UE) 2015/1535 del Parlament Europeu i del Consell.[5]

[5] En la nostra legislació estatal, és convenient consultar la Llei de serveis de la societat de la informació i comerç electrònic.

Organització internacional: una organització internacional i els ens subordinats de Dret internacional públic o qualsevol altre organisme creat mitjançant un acord entre dos o més països o en virtut de l'acord.

Són molts termes, alguns molt similars en concepte al que podem entendre'n en l'exercici de la professió informàtica, però altres dotats de característiques que els fan diferents al que se n'intueix, en considerar-los en el marc legal.

Altres definicions de molt d'interès:

Cessió o comunicació de dades: tota revelació de dades feta a una persona diferent de l'interessat. (Per exemple, amb finalitats publicitàries o entre empreses situades en diferents països.)

Fonts accessibles al públic: els fitxers la consulta dels quals la pot fer qualsevol persona, no impedida per una norma limitativa, o sense més exigència que, si escau, l'abonament d'una contraprestació. Tenen la consideració de fonts d'accés públic, exclusivament, el cens promocional,[6] els repertoris telefònics en els termes que preveu la normativa específica i les llistes de persones pertanyents a grups de professionals (sempre que hagen prestat el consentiment) que continguen únicament les dades de nom, títol, professió, activitat, grau acadèmic, direcció i indicació de pertànyer al grup. Així mateix, tenen el caràcter de fonts d'accés públic, els diaris i butlletins oficials i els mitjans de comunicació.

Drets

Quins drets té el ciutadà? Què indica la llei? Els nostres usuaris, clients, els nostres veïns, nosaltres, veiem com s'arrepleguen les nostres dades i en acabant es tracten. I amb les dades anem nosaltres. El procés recorda a alguns les llegendes que ens parlen d'aborígens que es negaven a ser fotografiats perquè així se'ls robava l'ànima. Bé, és possible que l'ànima no ens la roben, però el que sí que ens poden furtar és tot rastre de privacitat.

Sobre què hem de fer, un resum ens el dóna el RGPD en el considerant 59, en el qual llegim que s'han de facilitar, inclosos els mecanismes necessaris per a fer-ho, l'accés a les dades personals i la rectificació o supressió, així com l'exercici del dret d'oposició. A més, en el mateix considerant s'indica el termini màxim d'un mes per a atendre les peticions dels interessats... o justificar per què no les atén. Parlarem d'aquests drets, i d'uns altres amb no més poca importància. Comencem amb el dret d'accés, per a anar desgranant la resta en epígrafs successius.

Dret d'accés de l'interessat (article 15)

Els interessats han de tenir dret a accedir a les dades personals arreplegades que el concernisquen i a exercir el dit dret amb facilitat i a intervals raonables, amb la finalitat de

[6] No cal confondre el cens promocional (disponible per al públic) amb l'electoral ni amb el padró municipal (dades reservades, només amb finalitats estadístiques). El cens promocional només inclou nom, cognoms i adreça. A més, quant als mitjans de comunicació, vegeu en qualsevol periòdic que, així com la llista de morts inclou nom i cognoms, la llista de naixements és una nota simple amb el nom dels xiquets (sense cognom).

conèixer i verificar la licitud del tractament. Entre aquestes dades figuren les relatives a la salut (històries clíniques, etc.). Han de tenir el dret a conèixer i que se li comuniquen, en particular, les finalitats per a les quals es tracten les dades personals, el termini de tractament, els destinataris, la lògica implícita en tot tractament automàtic de dades personals i, almenys, quan es base en l'elaboració de perfils, les conseqüències d'aquest tractament. Cal considerar que aquest dret no ha d'afectar negativament els drets i llibertats de tercers, inclosos els secrets comercials o la propietat intel·lectual i, en particular, els drets de propietat intel·lectual que protegeixen programes informàtics (considerant 63).

L'interessat té dret a obtenir del responsable del tractament confirmació de si es tracten o no dades personals que el concerneixen i, en aquest cas, dret d'accés a les dades personals i a informacions com ara quines són les finalitats del tractament, les categories de dades personals de què es tracte; els destinataris, en particular si es tracta de tercers o organitzacions internacionals; el dret a presentar una reclamació davant d'una autoritat de control; l'origen de les dades, la possible existència de decisions basades en perfils...

El responsable pot percebre per qualsevol altra còpia sol·licitada per l'interessat un cànon raonable basat en els costos administratius. Quan l'interessat presente la sol·licitud per mitjans electrònics, i llevat que sol·licite que es facilite d'una altra manera, la informació s'ha de facilitar en un format electrònic d'ús comú.

Què en diu la LOPD?

L'afectat al qual es deneguen aquests drets pot posar-ho en coneixement de la direcció de l'Agència de Protecció de Dades, que s'assegurarà de la procedència o improcedència de la denegació. Aquest dret només es pot exercir en intervals superiors a dotze mesos, llevat que l'afectat acredite un interès legítim, cas en el qual es pot exercir abans.

Dret de rectificació (article 16)

L'interessat té dret a obtenir sense dilació indeguda del responsable del tractament la rectificació de les dades personals inexactes que el concernisquen. L'interessat té dret que es completen les dades personals que siguen incompletes.

Què en diu la LOPD?

La rectificació l'ha de fer efectiva el responsable del fitxer dins dels cinc dies següents al de la recepció de la sol·licitud. Si les dades rectificades o cancel·lades s'hagueren cedit prèviament, el responsable del fitxer ha de notificar la rectificació o cancel·lació efectuada al cessionari en el termini de cinc dies. Si el titular considera que no procedeix accedir al que se sol·licita li ho ha de comunicar motivadament en el termini de cinc dies. Si transcorregut el termini de cinc dies no contesta, es pot entendre la petició com a desestimada.

Dret de supressió (article 17), anomenat també dret a l'oblit

Garriga el defineix com a cancel·lació de dades personals que ja no siguen necessàries per a la realització del propòsit concret que en va motivar l'arreplega i el tractament (Garriga Domínguez, 2010).

Els considerants 65 i 66 ens defineixen aquest dret important, una de les novetats respecte de la legislació anterior. Així, podem llegir que els interessats han de tenir dret que les seues dades personals se suprimisquen i deixen de tractar-se si ja no són necessàries per a les finalitats per a les quals es van arreplegar, o tractades d'una altra manera, si els interessats n'han retirat el consentiment per al tractament o s'oposen al tractament de dades personals que els concerneixen, o si el tractament de les dades personals incompleix d'una altra manera el reglament.

Hi aprofundeix indicant que és particularment pertinent quan el consentiment es va donar sent xiquet, per no tenir la plenitud de la consciència sobre els riscos que implica el tractament. En concret, assenyala la necessitat de suprimir aquestes dades personals en internet. És una ampliació de drets preexistents, de manera que es reforça referent a les dades publicades en internet, de manera que el responsable del tractament que haja fet públiques dades personals estiga obligat a indicar als responsables del tractament que tracten aquestes dades personals que suprimisquen tot enllaç a questes dades, o les còpies o rèpliques, cosa que cal fer considerant possibles canvis en la tecnologia.

Òbviament hi ha excepcions, entre les quals destaquen les que indiquen que són necessàries per al compliment d'una obligació legal, per al compliment d'una missió feta en interès públic (inclòs l'àmbit de la salut), amb finalitats d'arxiu, investigació científica o històrica o estadístiques. De la mateixa manera es fa l'excepció pertinent per a quan és precisa la conservació de cara a l'exercici o defensa de reclamacions.

El precedent clar l'hem de cercar en l'activitat del tribunal europeu en defensa dels ciutadans, fet que podem particularitzar en la sentència del 13 de maig del 2014 de la Gran Sala del Tribunal de Justícia en el cas del ciutadà espanyol M. C. contra Google, en la qual, en les declaracions finals podem llegir que:

«[…] el gestor d'un motor de cerca està obligat a eliminar de la llista de resultats obtinguda després d'una cerca feta a partir del nom d'una persona vincles a pàgines web, publicades per tercers i que contenen informació relativa a la dita persona, també en el cas que aquest nom o aquesta informació no s'esborren prèviament o simultàniament d'aquestes pàgines web, i, si escau, encara que la publicació en aquestes pàgines siga en si mateixa lícita» (Gran Sala del Tribunal de Justícia, 2014).

Pregunta: com afectaria això a una hemeroteca virtual històrica, com ara la Biblioteca Virtual de Premsa Històrica? (Secretaria de Estado de Cultura)

Vegeu la notícia «El Constitucional extiende el derecho al olvido a las hemerotecas digitales» (Rincón, 2018)

Dret a la limitació del tractament (article 18)

Seguint el reglament, s'han d'incloure entre els mètodes per a limitar el tractament de dades personals el de 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 d'internet.

Destaca l'al·lusió als fitxers automatitzats en els quals la limitació del tractament s'ha de fer per mitjans tècnics, de manera que les dades personals no siguen objecte d'operacions de tractament ulterior ni es puguen modificar. (considerant 67)

Quan es pot exercir aquest dret?

- Quan s'impugne l'exactitud de les dades personals, durant el termini en què el responsable puga verificar-ne l'exactitud;
- quan l'interessat s'opose a la supressió de les dades personals i sol·licite en el seu lloc la limitació d'ús;
- quan el responsable ja no necessite les dades personals per a les finalitats del tractament, però l'interessat les necessite per a la formulació, l'exercici o la defensa de reclamacions.

El responsable ha d'informar l'interessat abans de l'alçament d'aquesta limitació.

A més, el responsable del tractament ha de comunicar qualsevol rectificació o supressió de dades personals o limitació del tractament a cada un dels destinataris als quals s'hagen comunicat les dades personals, llevat que siga impossible o exigisca un esforç desproporcionat. (article 19)

Dret a la portabilitat (article 20)

És el dret de l'interessat a rebre les dades personals que l'incumbisquen, que haja facilitat a un responsable del tractament, en un format estructurat, d'ús comú i lectura mecànica, i a transmetre-les a un altre responsable del tractament sense que ho impedisca el responsable al qual s'hagen facilitat.

És un dret que pot ser molt útil en canviar de companyia de subministraments (telèfon, per exemple) o de faena.

En exercir el dret a la portabilitat de les dades, l'interessat té dret que les dades personals es transmeten directament de responsable a responsable quan siga tècnicament possible. Per exemple, en canviar de companyia de telèfon, l'interessat només ha de demanar la portabilitat, i és la companyia que rep la petició l'encarregada dels tràmits de baixa de la línia anterior.

No s'aplica al tractament necessari per al compliment d'una missió feta en interès públic o en l'exercici de poders públics conferits al responsable del tractament.

Dret d'oposició (article 21)

És el dret de l'interessat a oposar-se en qualsevol moment, per motius relacionats amb la seua situació particular, al fet que dades personals que el concernisquen siguen objecte d'un tractament, inclosa l'elaboració de perfils sobre la base d'aquestes disposicions.

Ha de ser el responsable el que demostre que els interessos legítims imperiosos que té prevalen sobre els interessos o els drets i llibertats fonamentals de l'interessat. (considerant 69)

Quan el tractament de dades personals tinga com a objecte el màrqueting directe, l'interessat té dret a oposar-se en tot moment al tractament de les dades personals que el concernisquen, inclosa l'elaboració de perfils.

L'interessat pot exercir el dret a oposar-s'hi per mitjans automatitzats que apliquen especificacions tècniques.

Quan les dades personals es tracten amb finalitats d'investigació científica o històrica o finalitats estadístiques, l'interessat té dret, per motius relacionats amb la seua situació particular, a oposar-se al tractament de dades personals que el concernisquen, llevat que siga necessari per al compliment d'una missió feta per raons d'interès públic.

Decisions individuals automatitzades (elaboració de perfils) (article 22)

Parlem ara del dret de no ser objecte d'una decisió que avalue aspectes personals, i que es base únicament en el tractament automatitzat i produïsca efectes jurídics o afecte significativament l'interessat (per exemple, la denegació automàtica d'un crèdit sense intervenció humana). Es

tracta d'avaluar (o de no fer-ho) aspectes personals relatius a una persona física, per a analitzar o predir aspectes relacionats amb el rendiment en la faena, la situació econòmica, la salut, les preferències o els interessos personals, la fiabilitat o el comportament, la situació o els moviments de l'interessat... (vegeu per exemple la pel·lícula documental *Sicko* de Michael Moore (2007).[7] D'altra banda, sí que es permeten les decisions basades en aquest tractament, inclosa l'elaboració de perfils, si ho autoritza expressament el Dret de la Unió o dels Estats membres, per exemple per al control i la prevenció del frau i l'evasió fiscal, i per a garantir la seguretat i la fiabilitat d'un servei prestat, o quan és necessari per a la conclusió o execució d'un contracte entre l'interessat i un responsable del tractament, o en els casos en els quals l'interessat haja donat el consentiment explícit. Les garanties d'aquest tractament de qualsevol forma s'han de cenyir a les garanties apropiades (donar informació específica a l'interessat; dret a obtenir intervenció humana; dret a expressar el punt de vista; dret a rebre una explicació de la decisió presa i a impugnar la decisió). En tot cas no ha d'afectar un menor.

El responsable del tractament ha d'utilitzar procediments matemàtics o estadístics adequats per a l'elaboració de perfils, aplicar mesures tècniques i organitzatives apropiades per a garantir la correcció d'inexactituds i reducció del risc d'error, impedint efectes discriminatoris en les persones físiques per motius de raça o origen ètnic, opinions polítiques, religió o creences, afiliació sindical, condició genètica o estat de salut o orientació sexual. Les decisions automatitzades i l'elaboració de perfils sobre la base de categories particulars de dades personals únicament s'han de permetre en condicions específiques. (considerant 71)

Quines limitacions tenen aquests drets? (article 23) (considerant 19)

Els Estats membres poden encomanar a les autoritats competents (vegeu la Directiva Europea 2016/680 del Parlament Europeu i del Consell, de 27 d'abril del 2016, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les autoritats competents per a finalitats de prevenció) funcions que no es duguen a terme necessàriament amb finalitats de prevenció, investigació, detecció o enjudiciament d'infraccions penals o execució de sancions penals, inclosa la protecció per amenaces a la seguretat pública i prevenció d'amenaces, indicant-se expressament que els Estats membres puguen, en condicions específiques, limitar d'acord amb el dret determinades obligacions i drets sempre que siga una mesura necessària i proporcionada en una societat democràtica per a protegir interessos específics importants.

Això implica que s'han de respectar en allò essencial els drets i llibertats fonamentals, malgrat les excepcions que han de ser sempre «mesures necessàries i proporcionades».

Sobre els interessos específics importants es destaquen la prevenció, investigació, detecció o enjudiciament d'infraccions penals o l'execució de sancions penals; interessos econòmics o financers importants de la Unió o d'un Estat membre, inclusivament en els àmbits fiscal, pressupostari i monetari, la sanitat pública i la seguretat social; la protecció de la independència judicial; la prevenció, la investigació, la detecció i l'enjudiciament d'infraccions de normes

[7] Es tracta d'una visió molt crítica sobre el sistema de salut dels Estats Units, en concret sobre les companyies sanitàries privades enfront d'un sistema de salut públic com els que tenim en uns quants països europeus.

deontològiques en les professions regulades; la protecció de l'interessat o dels drets i llibertats d'uns altres.

Figures professionals i actors que s'hi han de considerar

Responsable del tractament (article 24)

Aquesta figura està definida en l'apartat de definicions, però faltava encara perfilar-ne el rol.

Considerant naturalesa, àmbit, context, finalitats del tractament i riscos, el responsable del tractament ha d'aplicar, revisar i actualitzar mesures tècniques i organitzatives apropiades a fi de garantir i poder demostrar que el tractament és conforme al reglament. L'adhesió a codis de conducta o a un mecanisme de certificació es poden utilitzar com a elements per a demostrar el compliment de les obligacions per part del responsable del tractament.

Per a determinar si el dit responsable (o encarregat, si escau, perquè està subjecte a les mateixes condicions) ofereix béns o serveis a interessats que residisquen a la Unió, s'ha de determinar si és evident que el responsable o l'encarregat projecta oferir serveis a interessats en un o diversos dels Estats membres de la Unió. Si bé la mera accessibilitat del lloc web del responsable o encarregat o d'un intermediari a la Unió, d'una adreça de correu electrònic o altres dades de contacte, o l'ús d'una llengua generalment utilitzada en el tercer país on residisca el responsable del tractament, no n'hi ha prou per a determinar aquesta intenció, hi ha factors, com l'ús d'una llengua o una moneda utilitzada generalment en un o diversos Estats membres amb la possibilitat d'encarregar béns i serveis en aquesta altra llengua, o l'esment de clients o usuaris que resideixen a la Unió, que poden revelar que el responsable del tractament projecta oferir béns o serveis a interessats a la Unió. (considerant 23)

Corresponsables del tractament (article 26)

Es dona quan dos o més responsables determinen conjuntament els objectius i els mitjans del tractament. En aquest cas, han de determinar de manera transparent i de mutu acord les responsabilitats respectives. S'han de posar a la disposició de l'interessat els aspectes essencials de l'acord.

Representants de responsables o encarregats no establits a la Unió (article 27)

Es designa per escrit un representant a la Unió. Però això no s'aplica si el tractament és ocasional, no inclou maneig a gran escala de categories especials de dades i és improbable que comporte un risc per als drets i llibertats de les persones físiques o a les autoritats o organismes públics.

Aquesta designació d'un representant pel responsable o l'encarregat del tractament s'ha d'entendre sense perjudici de les accions que es puguen emprendre contra el responsable o encarregat.

Encarregat del tractament (article 28, 29)

Igual que amb el responsable del tractament, aquesta figura està definida en l'apartat de definicions, però faltava encara perfilar-ne el rol.

En fer un tractament per compte d'un responsable del tractament, ha de triar únicament un encarregat que oferisca garanties suficients per a aplicar mesures tècniques i organitzatives apropiades. L'encarregat del tractament no ha de recórrer a un altre encarregat sense l'autorització prèvia per escrit, específica o general, del responsable.

Per a garantir el compliment del present reglament, el responsable, en encomanar activitats de tractament a un encarregat, ha de recórrer únicament a encarregats que oferisquen garanties suficients, en particular pel que fa a coneixements especialitzats, fiabilitat i recursos, de cara a l'aplicació de mesures tècniques i organitzatives que complisquen els requisits del reglament, inclosa la seguretat del tractament. (considerant 81)

El tractament per l'encarregat s'ha de regir per un contracte que vincule l'encarregat respecte del responsable i establisca l'objecte, la durada, la naturalesa i la finalitat del tractament, el tipus de dades personals i categories d'interessats, i les obligacions i drets del responsable. Aquest contracte ha d'estipular, entre altres coses, que l'encarregat tracta les dades personals únicament seguint instruccions documentades del responsable (incloses transferències a un país tercer); ha de garantir que les persones autoritzades per a tractar dades personals s'hagen compromès a respectar la confidencialitat; ha d'assistir el responsable, tenint en compte la naturalesa del tractament, a través de mesures tècniques i organitzatives apropiades, sempre que siga possible, perquè puga complir l'obligació que té de respondre a les sol·licituds; a tria del responsable, ha de suprimir o retornar totes les dades personals una vegada finalitze la prestació dels serveis de tractament, i suprimir-ne les còpies existents llevat que es requerisca la conservació de les dades personals; ha de posar a la disposició del responsable tota la informació necessària per a demostrar el compliment de les obligacions establides, tot permetent la realització d'auditories i contribuint-hi.

L'encarregat del tractament assisteix el responsable quan siga necessari i a petició seua, a fi d'assegurar que es compleixen les obligacions que es deriven de la realització de les avaluacions d'impacte relatives a la protecció de dades i de la consulta prèvia a l'autoritat de control. (considerant 95)

L'adhesió de l'encarregat del tractament a un codi de conducta o a un mecanisme de certificació es pot utilitzar com a element per a demostrar l'existència de les garanties suficients.

Sobre el contracte que vincula el responsable amb l'encarregat, cal indicar que l'autoritat de control pot adoptar clàusules contractuals tipus. El contracte ha de constar per escrit, inclusivament en format electrònic. Si un encarregat del tractament infringeix el reglament en determinar les finalitats i els mitjans del tractament, es considera responsable del tractament respecte a aquest tractament.

Proposta:

Localitza clàusules contractuals tipus en la web de l'Agència Espanyola de Protecció de Dades (2018).

El contracte ha de fixar l'objecte i la durada del tractament, la naturalesa i les finalitats del tractament, el tipus de dades personals i les categories d'interessats, tenint en compte les

funcions i les responsabilitats específiques de l'encarregat en el context del tractament que s'ha de dur a terme i del risc per als drets i llibertats de l'interessat. (considerant 81)

L'encarregat del tractament i qualsevol persona que actue sota la seua autoritat o la de l'encarregat i tinga accés a dades personals només podran tractar aquestes dades seguint instruccions del responsable.

Una vegada finalitzat el tractament per compte del responsable, l'encarregat ha de, a tria d'aquell, retornar o suprimir les dades personals, llevat que el Dret de la Unió o dels Estats membres aplicable a l'encarregat del tractament obligue a conservar les dades. (considerant 81)

Cal destacar que tant responsable com encarregat del tractament i els representants han de cooperar amb l'autoritat de control que ho sol·licite en l'acompliment de les seues funcions. (article 31)

Delegat de protecció de dades (article 37, 38)

El «delegat de protecció de dades» és una figura que s'incorpora amb el reglament a les ja existents d'encarregat o responsable (tot i que en la legislació alemanya ja existia), ha de ser un especialista en dret de protecció de dades, amb unes funcions que fan que parega una mena de defensor del poble de les dades. Les funcions serien, bàsicament (article 39):

- Informar i assessorar els responsables i encarregats del tractament de dades personals (i els empleats) de les obligacions que tenen, derivades de la legislació.
- Supervisar el compliment de la legislació i de la política interna de protecció de dades d'una administració pública o empresa.
- Quan se li sol·licite, assessorar sobre l'avaluació d'impacte d'un tractament de dades personals (sobre aquest interessant element tornarem), quan comporte un risc alt per als drets i les llibertats de les persones físiques, i supervisar-ne l'aplicació després.
- Cooperar amb les «autoritats de control» (això és, amb les agències de protecció de dades).
- Servir de finestreta o de punt de contacte de les autoritats de control per a qualsevol consulta sobre el tractament de dades personals.

Al contrari que les figures anteriors no sempre ha d'existir. Només fa falta quan el tractament el du a terme una autoritat o organisme públic (excepte tribunals), o quan les operacions de tractament en raó de la naturalesa, abast i/o finalitats, requerisquen una observació habitual i sistemàtica d'interessats a gran escala, o si consisteixen en el tractament a gran escala de categories especials de dades personals i de dades relatives a condemnes i infraccions penals.

En resum: fa falta un delegat si es tracta d'un tractament des de l'administració pública, quan es treballa amb dades d'un nombre de persones elevat, o quan es treballa amb un nombre de dades especials elevat.

Quines característiques ha de complir un delegat de protecció de dades? S'hi valoren les qualitats professionals, en particular, els coneixements especialitzats del dret i la pràctica en matèria de protecció de dades i la capacitat que té per a exercir les funcions. Ha d'exercir les seues funcions prestant l'atenció deguda als riscos associats a les operacions de tractament, tenint en compte la naturalesa, l'abast, el context i les finalitats del tractament.

El nivell de coneixements especialitzats necessari s'ha de determinar en funció de les operacions de tractament de dades que es duguen a terme i de la protecció exigida per a les dades personals tractades pel responsable o l'encarregat. (considerant 97)

Pot formar part de la plantilla del responsable o de l'encarregat del tractament o exercir-ne les funcions en el marc d'un contracte de serveis.

El responsable i l'encarregat del tractament han de garantir que el delegat de protecció de dades participe de manera adequada i en temps oportú en totes les qüestions relatives a la protecció de dades personals. Li han de facilitar els recursos necessaris per a l'acompliment de les funcions que té i l'accés a les dades personals i a les operacions de tractament, i per al manteniment dels seus coneixements especialitzats, garantint que no rep cap instrucció pel que fa a l'acompliment de les seues funcions. Ret comptes directament al nivell jeràrquic més alt del responsable o encarregat.

Els interessats es poden posar en contacte amb ell pel que fa a totes les qüestions relatives al tractament de les seues dades personals i a l'exercici dels seus drets. Està obligat a mantenir-ne el secret, encara que pot exercir altres funcions i comeses (que no han de donar lloc a conflicte d'interessos).

El treball del professional de la informació

Parlarem en aquest apartat de les tasques que ha de dur a terme el professional, en alguns dels rols més destacats: responsable o encarregat del tractament, delegat de dades…

Hi ha elements que s'han de dur a terme amb la màxima diligència, com el registre de les activitats de tractament, l'avaluació d'impacte, l'atenció als drets dels usuaris… Anirem desgranant-ne els més importants.

Subratllem un dels canvis principals: l'actitud del professional ha de ser proactiva. No hi ha prou de complir la llei, cal demostrar que s'ha posat tot el possible per part seua per complir-la.

Registre de les activitats de tractament (article 30)

Cada responsable ha de portar un registre de les activitats de tractament fetes sota la seua responsabilitat. La primera pregunta pot ser: què ha de contenir aquest registre?

- nom i les dades de contacte del responsable (i corresponsable), del representant del responsable, i del delegat de protecció de dades;
- les finalitats del tractament;
- descripció de les categories d'interessats i de les categories de dades personals;
- categories de destinataris a qui es van comunicar o es comunicaran les dades personals;
- si n'hi ha, les transferències de dades personals a un país tercer;
- quan siga possible, els terminis previstos per a la supressió de les diferents categories de dades;
- quan siga possible, una descripció general de les mesures tècniques i organitzatives de seguretat.

Al seu torn, cada encarregat ha de dur a terme un registre de totes les categories d'activitats de tractament fetes per compte d'un responsable que ha de contenir:

- nom i les dades de contacte de l'encarregat o encarregats i de cada responsable per compte del qual actue l'encarregat, i, si escau, del representant del responsable o de l'encarregat, i del delegat de protecció de dades;
- categories de tractaments fets per compte de cada responsable;
- si n'hi ha, transferències de dades personals a un país tercer;
- quan siga possible, una descripció general de les mesures tècniques i organitzatives de seguretat.

Aquests registres, d'encarregat i responsable, han de constar per escrit i s'ha de posar a la disposició de l'autoritat de control que ho sol·licite. Cal indicar que no són aplicables a cap empresa ni organització de menys de 250 persones, llevat que el tractament que en faça puga comportar un risc per als drets i llibertats dels interessats, no siga ocasional, o incloga categories especials de dades personals.

Amb el reglament desapareix l'obligació de notificar la inscripció de fitxers, tant de responsables públics o privats, en el Registre de Fitxers de l'AEPD, o registre de l'autoritat autonòmica competent, sense perjudici de l'obligació d'implementar el Registre d'Activitats de Tractament.

Quina informació s'ha de facilitar? (articles 13 i 14)

Destaquem els elements següents:

- la identitat i les dades de contacte del responsable i, si escau, del representant;
- les dades de contacte del delegat de protecció de dades, si escau;
- les finalitats del tractament a què es destinen les dades personals i la base jurídica del tractament;
- els destinataris o categories de destinataris de les dades personals;
- la intenció del responsable de transferir dades personals a un país tercer o organització internacional;
- el termini durant el qual s'han de conservar les dades personals o, quan no siga possible, els criteris utilitzats per a determinar aquest termini;
- l'existència del dret a sol·licitar al responsable del tractament l'accés, rectificació o supressió, limitació, oposició i portabilitat de les dades;
- el dret a presentar una reclamació davant d'una autoritat de control;
- l'existència de decisions automatitzades, inclosa l'elaboració de perfils;
- quan el responsable del tractament projecte el tractament ulterior de dades personals per a una finalitat que no siga aquella per a la qual es van arreplegar, ha de proporcionar a l'interessat, amb anterioritat a aquest tractament, informació sobre el tractament.

Què s'ha de facilitar quan les dades personals s'obtenen de l'interessat? (article 13)

És important ressenyar que en aquest cas hem d'indicar si la comunicació de dades personals és un requisit legal o contractual, o un requisit necessari per a firmar un contracte.

Què s'ha de facilitar quan les dades personals no s'obtenen de l'interessat? (article 14)

Cal afegir-hi en aquest cas la font de la qual procedeixen les dades personals i, si escau, si procedeixen de fonts d'accés públic.

Cal afegir-hi que dins d'un termini raonable, a tot tardar en un mes des d'obtenir les dades personals s'ha de comunicar si s'han de fer servir per a la comunicació amb l'interessat (això com a més tard en la primera comunicació) i, si hi ha previst comunicar-les a un altre destinatari, a tot tardar en el moment en què les dades personals es comuniquen per primera vegada.

Tot això no és aplicable si l'interessat ja disposa de la informació o comunicar-la suposa un esforç desproporcionat, sobretot quan es tracte de tractament amb finalitats d'arxiu en interès públic (investigació científica, històrica o finalitats estadístiques); o bé si l'obtenció o comunicació està expressament establida pel Dret de la Unió o dels Estats membres, o quan les dades personals hagen de continuar tenint caràcter confidencial sobre la base d'una obligació de secret professional regulada pel Dret de la Unió o dels Estats membres.

Com s'han de donar les dades que es faciliten?

Les dades s'han de facilitar en un format estructurat, d'ús comú, de lectura mecànica i interoperable. Per això, des dels Estats s'encoratja els responsables a crear formats interoperables que permeten la portabilitat de dades. El dret de l'interessat a transmetre o rebre dades personals que el concernisquen no ha d'obligar el responsable a adoptar o mantenir sistemes de tractament que siguen tècnicament compatibles.

I si se'ns demana que suprimim dades? Hi ha una consideració clau: no ha d'implicar la supressió de les dades personals concernents a l'interessat que haja facilitat per a l'execució d'un contracte, en la mesura i durant el temps en què les dades personals siguen necessàries per a l'execució del dit contracte. (considerant 68)

Seguretat del tractament (article 32)

El reglament obliga que, considerant l'estat de la tècnica, els costos d'aplicació i la naturalesa, l'abast, el context i les finalitats del tractament, així com riscos de probabilitat i gravetat variables per als drets i llibertats de les persones físiques, el responsable i l'encarregat apliquen mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat al risc.[8]

Aquestes mesures passen per fer servir:

- la pseudonimització i l'encriptació de dades personals;
- la capacitat de garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament;
- la capacitat de restaurar la disponibilitat i l'accés a les dades personals de manera

[8] És molt difícil avaluar-ne el risc. Posem dos exemples de ciberatacs amb robatori de dades personals. D'una banda, un atac d'Anonymous en el qual es van emportar més de 200 GB d'informació de la base de dades de Stratfor Global, companyia especialitzada en seguretat, amb informació dels clients (números de targetes de crèdit, adreces i correus electrònics). Era previsible? Potser per la visibilitat de l'empresa. Què va succeir amb les dades? L'important ací és la pregunta «què hi podria passar?». I la resposta és esborronadora. Davant d'aquest cas de dimensions quasi globals, en trobem d'altres més d'anar per casa, com aquell centre de salut que va veure filtrades les dades de 1.700 pacients per mitjà del programa emule en les xarxes P2P. Un abast menor, amb dades molt sensibles. Com es pot evitar?

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 a garantir la seguretat del tractament.

Els riscos que es marquen com més preocupants són la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o accés no autoritzats a les dades.

Els riscos per als drets i llibertats de les persones físiques, de gravetat i probabilitat variables es poden deure del tractament de dades que pogueren provocar danys i perjudicis físics, materials o immaterials, en particular en els casos en els quals el tractament puga donar lloc a problemes de discriminació, usurpació d'identitat o frau, pèrdues financeres, mal per a la reputació, pèrdua de confidencialitat de dades subjectes al secret professional, reversió no autoritzada de la pseudonimització o qualsevol altre perjudici econòmic o social significatiu; en els casos en els quals es prive els interessats dels drets i llibertats o se'ls impedisca exercir el control sobre les seues dades personals; en els casos en els quals les dades personals tractades revelen l'origen ètnic o racial, les opinions polítiques, la religió o creences filosòfiques, la militància en sindicats i el tractament de dades genètiques, dades relatives a la salut o dades sobre la vida sexual, o les condemnes i infraccions penals o mesures de seguretat connexes; en els casos en els quals s'avaluen aspectes personals, en particular l'anàlisi o la predicció d'aspectes referits al rendiment en el treball, situació econòmica, salut, preferències o interessos personals, fiabilitat o comportament, situació o moviments, amb la finalitat de crear o utilitzar perfils personals; en els casos en els quals es tracten dades personals de persones vulnerables, en particular xiquets; o en els casos en els quals el tractament implique una gran quantitat de dades personals i afecte un gran nombre d'interessats (considerant 75).

Els danys i perjudicis físics, materials o immaterials per a les persones físiques són variats i de diferent abast: pèrdua de control sobre les dades personals o restricció dels drets, discriminació, usurpació d'identitat, pèrdues financeres, reversió no autoritzada de la pseudonimització, perjuí per a la reputació, pèrdua de confidencialitat de dades subjectes al secret professional, o qualsevol altre perjudici econòmic o social significatiu per a la persona física en qüestió. (considerant 85). Hi veiem una correlació òbvia entre els riscos emmarcats en el requadre superior i els danys enumerats ací.

Les persones físiques es poden associar a identificadors en línia facilitats pels seus dispositius, aplicacions, eines i protocols, com ara adreces dels protocols d'internet, identificadors de sessió en forma de *cookies* o altres identificadors, com ara etiquetes d'identificació per radiofreqüència. Això pot deixar empremtes que, en particular, en ser combinades amb identificadors únics i altres dades rebudes pels servidors, es poden utilitzar per a elaborar perfils de les persones físiques i identificar-les. (considerant 30)

Quan es produeix una violació de la seguretat de les dades personals cal notificar-ho a l'autoritat de control (article 33) (i, per descomptat, a l'interessat; article 34). Els terminis en tots dos casos són molt breus i en el contingut de la notificació ha de figurar, de cara a l'autoritat de control:

1. la naturalesa de la violació de la seguretat de les dades personals, inclusivament, quan siga possible, les categories i el nombre aproximat d'interessats afectats, i les

categories i el nombre aproximat de registres de dades personals afectats;

2. comunicar el nom i les dades de contacte del delegat de protecció de dades o d'un altre punt de contacte en el qual se'n puga obtenir més informació;
3. descriure les possibles conseqüències de la violació de la seguretat de les dades personals;
4. descriure les mesures que adopta o proposa el responsable del tractament per a posar remei a la violació de la seguretat de les dades personals, incloses, si escau, les mesures adoptades per a mitigar els possibles efectes negatius.

De cara a l'interessat, si és previsible una violació de la seguretat, el responsable l'ha de comunicar a l'interessat sense dilació indeguda (descrivint amb llenguatge clar i senzill la naturalesa de la violació de la seguretat i les mesures que s'hi han de prendre). Aquesta comunicació no és necessària si el responsable del tractament ha adoptat mesures de protecció tècniques i organitzatives apropiades i les dades resulten inintel·ligibles (encriptació), o si s'han pres mesures ulteriors que garantisquen que eliminen el risc; o si la comunicació suposa un esforç desproporcionat, en aquest cas se'n pot fer una comunicació pública. Destaquem que les comunicacions als interessats s'han de fer tan prompte com siga raonablement possible i en cooperació estreta amb l'autoritat de control, seguint-ne les orientacions o les d'altres autoritats competents, com les autoritats policials (considerant 86).

Tota violació de la seguretat l'ha de documentar el responsable del tractament.

I el secret professional?

Els Estats membres poden adoptar normes específiques per a fixar els poders de les autoritats de control en relació amb els responsables o encarregats subjectes a una obligació de secret professional, quan siga necessari. Aquestes normes només s'han d'aplicar a les dades personals rebudes en ocasió d'una activitat coberta per l'obligació de secret. (article 90)

Procurant un equilibri entre allò tècnicament possible a cada moment, i els riscos que té el tractament de dades, el responsable del tractament ha d'aplicar, tant en el moment de determinar els mitjans de tractament com en el moment del tractament, mesures tècniques i organitzatives apropiades, com ara la pseudonimització o la minimització de dades. Només han de ser objecte de tractament les dades personals que siguen necessàries per a cada una de les finalitats específiques del tractament, la qual cosa s'ha d'entendre tant, quant a l'extensió del tractament, com al termini de conservació i a l'accessibilitat. Això és el que entenem per protecció de dades des del disseny i per defecte (article 25).[9]

Tractament que no requereix identificació: si les finalitats per a les quals un responsable tracta dades personals no requereixen identificació d'un interessat pel responsable, no està obligat a mantenir, obtenir o tractar informació addicional amb vista a identificar l'interessat amb l'única

[9] Aquest principi de privacitat des del disseny (article 25.1) significa que en el disseny d'aplicacions que tracten dades personals, se n'ha de garantir la privacitat des del principi. Això implica, per exemple, que en matèria de xarxes socials, els perfils de privacitat dels usuaris estaran per defecte tancats a altres usuaris, i ha de ser l'usuari qui els òbriga a altri.

finalitat de complir el reglament. Si és capaç de demostrar que no està en condicions d'identificar l'interessat, l'ha d'informar, si és possible. (article 11)

Com i quan es fa una avaluació d'impacte relativa a la protecció de dades? (article 35)

Els tractaments de dades fan servir tècniques canviants en el temps. Sovint, ens trobem problemes, amb forats de seguretat, que resulten absolutament inesperats. Altres vegades, hi ha indicis que ens avisen per on poden venir els problemes.

Ja que és probable que les operacions de tractament comporten un risc alt per als drets i les llibertats de les persones físiques, el responsable ha de fer una avaluació d'impacte que avalue l'origen, la naturalesa, la particularitat i la gravetat del risc.

El resultat de l'avaluació s'ha de tenir en compte quan es decidisquen les mesures adequades que s'hagen de prendre amb la finalitat de demostrar que el tractament de les dades personals és correcte (considerant 84). S'ha de fer abans del tractament, amb l'assessorament del delegat de protecció de dades, si n'hi ha.

L'avaluació és imprescindible que es faça si es fa una avaluació sistemàtica i exhaustiva d'aspectes personals de persones físiques que es base en un tractament automatitzat, com l'elaboració de perfils, i sobre la base dels quals es prenguen decisions que produïsquen efectes jurídics per a les persones físiques o que els afecten significativament de manera similar; si es tracta de tractament a gran escala de les categories especials de dades, o si es fa una observació sistemàtica a gran escala d'una zona d'accés públic.

Les operacions de tractament en les quals s'han d'aplicar són aquelles a gran escala que persegueixen tractar una quantitat considerable de dades personals a escala regional, nacional o supranacional i que podrien afectar un gran nombre d'interessats i comporten probablement un risc alt, per exemple, a causa de la sensibilitat de les dades, quan, en funció del nivell de coneixements tècnics aconseguit, s'haja utilitzat una nova tecnologia a gran escala i en altres operacions de tractament que comporten un risc alt per als drets i llibertats dels interessats, en particular quan aquestes operacions fan més difícil per als interessats l'exercici dels seus drets.

L'avaluació d'impacte relativa a la protecció de dades s'ha de fer també en els casos en els quals es tracten dades personals per a adoptar decisions relatives a persones físiques concretes arran d'una avaluació sistemàtica i exhaustiva d'aspectes personals propis de persones físiques, basada en l'elaboració de perfils d'aquestes dades o arran del tractament de categories especials de dades personals, dades biomètriques o dades sobre condemnes i infraccions penals o mesures de seguretat connexes.

També és necessària una avaluació d'impacte relativa a la protecció de dades per al control de zones d'accés públic a gran escala, en particular quan s'utilitzen dispositius optoelectrònics[10] o per a qualsevol altre tipus d'operació quan l'autoritat de control competent considere que el

[10] En el reglament apareix un únic esment als dispositius optoelectrònics. Com és lògic, hi ha dispositius d'aquesta categoria, com els que indiquen quan s'esgota la bateria d'un dispositiu, que no tenen interès per a nosaltres, però altres, com els sensors que detecten amb alta fiabilitat la presència d'objectes i avaluen i permeten la generació d'informes sobre forma, color, distància o gruix, amb una fidelitat molt més gran que detectors de proximitat de tecnologia inductiva o capacitiva, tenen un risc evident quan aquests «objectes» són en realitat «persones».

tractament comporte probablement un risc alt per als drets i llibertats dels interessats, en particular perquè impedeix als interessats exercir un dret o utilitzar un servei o executar un contracte, o perquè s'efectua sistemàticament a gran escala.

El tractament de dades personals no s'ha de considerar a gran escala si el du a terme, respecte de dades personals de pacients o clients, un sol metge, un altre professional de la salut o advocat. En aquests casos, l'avaluació d'impacte de la protecció de dades no ha de ser obligatòria. (considerant 91)

Quines operacions són les que necessiten d'una avaluació d'impacte? L'autoritat de control les estableix i publica en una llista. També pot publicar la llista dels tipus de tractament que no requereixen avaluacions d'impacte relatives a la protecció de dades. Això implica que el professional ha d'estar permanentment informat consultant la web de l'autoritat de control, l'Agència Espanyola de Protecció de Dades en el nostre cas.

L'avaluació ha d'incloure com a mínim:

1. una descripció sistemàtica de les operacions de tractament previstes i de les finalitats del tractament, inclusivament l'interès legítim que persegueix el responsable del tractament;
2. una avaluació de la necessitat i la proporcionalitat de les operacions de tractament pel que fa a la finalitat que tenen;
3. una avaluació dels riscos per als drets i llibertats dels interessats;
4. les mesures previstes per a afrontar els riscos, incloses garanties, mesures de seguretat i mecanismes que garantisquen la protecció de dades personals.

El compliment dels codis de conducta pels responsables o encarregats corresponents s'ha de tenir degudament en compte en avaluar les repercussions de les operacions de tractament, en particular a l'efecte de l'avaluació d'impacte relativa a la protecció de dades. Quan siga procedent, el responsable ha de recaptar l'opinió dels interessats o dels representants en relació amb el tractament previst.

Si cal, el responsable ha d'examinar si el tractament és conforme a l'avaluació d'impacte relativa a la protecció de dades, almenys quan hi haja un canvi del risc que representen les operacions de tractament (pensem, per exemple, en un canvi d'un algorisme que revisa una base de dades de clients, que en no estar previst per l'avaluació d'impacte, deixa al descobert nous riscos).

Si l'avaluació d'impacte mostra un risc alt, el responsable ha de consultar l'autoritat de control abans de procedir al tractament. Si l'autoritat considera que no s'ha identificat o mitigat prou el risc, en un termini de huit setmanes des de la sol·licitud de la consulta, s'ha d'assessorar per escrit el responsable, i si escau l'encarregat, termini ampliable sis setmanes, en funció de la complexitat del tractament. El responsable ha de facilitar a l'autoritat de control l'avaluació d'impacte relativa a la protecció de dades i informar l'autoritat de control de les responsabilitats respectives del responsable, els corresponsables i els encarregats, així com de les finalitats i els mitjans del tractament previst i les mesures i garanties establides. Si n'hi ha, també ha de facilitar les dades de contacte del delegat de protecció de dades; a més de qualsevol altra informació que sol·licite l'autoritat de control. (article 36)

Com ha d'actuar el professional davant la transparència?

Hem parlat de l'aparent incompatibilitat d'algunes lleis. Ja hem destacat com la protecció de dades i la llibertat d'expressió pareixen xocar, i alguna cosa avançàvem sobre la transparència. Òbviament, no podem fer transparent un tros de fusta, no podem revelar dades personals per a dir que no tenim secrets, sobretot perquè no seran els nostres secrets, sinó els dels propietaris de les dades.

Ara, filem encara més prim: hem de ser transparents en la nostra faena. Hem de fer veure com impedim que es veja el que la llei impedeix veure. Aquest travallengua té resposta en l'article 12 del reglament. I és molt interessant per estar íntimament lligat al punt que veurem tot seguit, un dels que desperta més preocupació entre els professionals: el consentiment.

L'interessat ha de conèixer l'existència de l'operació de tractament i les finalitats que té. El responsable del tractament ha de facilitar a l'interessat la informació complementària que siga necessària per a garantir un tractament lleial i transparent, considerant circumstàncies i context. Així mateix ha d'informar l'interessat de l'existència de l'elaboració de perfils i de les conseqüències d'aquesta elaboració. Si les dades personals s'obtenen dels interessats, també se'ls ha d'informar de si estan obligats a facilitar-les i de les conseqüències en cas que no ho feren. Aquesta informació es pot transmetre en combinació amb unes icones normalitzades que oferisquen, de manera fàcilment visible, intel·ligible i clarament llegible, una visió de conjunt adequada del tractament previst. Les icones que es presenten en format electrònic han de ser llegibles mecànicament. (considerant 60)

De molt d'interès: el responsable ha de tenir en compte la necessitat d'usar un llenguatge clar i senzill, en particular quan es dirigisca específicament a un xiquet.

¿Devem sempre donar la informació que se'ns demana de manera tangible o electrònica? No. No necessàriament ha de tenir un format electrònic o imprès, si la sol·licitud es fa de manera verbal, la resposta es pot donar de la mateixa manera, sempre que estiga prou acreditada la identitat del peticionari. Es pot sol·licitar que es facilite la informació addicional necessària per a confirmar la identitat de l'interessat, la qual cosa és lògica, per a evitar donar-li informació sobre les dades a qui no hauria de tenir-la. Quan l'interessat presente la sol·licitud per mitjans electrònics, la informació es facilitarà per mitjans electrònics quan siga possible, llevat que l'interessat sol·licite que es facilite d'una altra manera. La informació facilitada així com tota comunicació i qualsevol actuació han gratuïtes.

Quant als terminis, en un mes s'ha de donar resposta complida i, si per raons de complexitat o de nombre elevat de sol·licituds no és possible, es pot prorrogar dos mesos més, informant l'interessat de la pròrroga en el termini d'un mes a partir de la recepció de la sol·licitud, tot indicant els motius de la dilació. Si no dona curs a la sol·licitud i no informa de les raons de la seua no actuació, hi ha la possibilitat de presentar una reclamació davant d'una autoritat de control i d'exercir accions judicials. Si les sol·licituds són manifestament infundades o excessives (per exemple pel caràcter repetitiu), el responsable del tractament podrà cobrar un cànon raonable en funció dels costos administratius afrontats per a facilitar la informació o la comunicació o dur a terme l'actuació sol·licitada, o negar-se a actuar respecte de la sol·licitud. En tot cas, el responsable del tractament ha de suportar la càrrega de demostrar el caràcter manifestament infundat o excessiu de la sol·licitud.

Les dades dels treballadors. Tractament en l'àmbit laboral (article 88)

Una empresa no pot viure sense gestionar les dades dels seus treballadors. Això ha sigut així des de temps immemorials, motiu pel qual els diferents Estats han creat al llarg de les dècades les seues normes pròpies sobre el tema. Això, ho respecta el reglament indicant que podran establir normes més específiques per a garantir la protecció dels drets i llibertats en relació amb el tractament de dades personals dels treballadors en l'àmbit laboral, contemplant particularment que s'hi han d'incloure mesures específiques per a preservar la dignitat humana dels interessats així com els seus interessos legítims i els seus drets fonamentals, amb l'accent posat principalment en la transparència del tractament, la transferència de les dades personals dins d'un grup empresarial o d'una unió d'empreses dedicades a una activitat econòmica conjunta i en els sistemes de supervisió en el lloc de treball.

Què fem amb el correu electrònic dels treballadors? A priori, llegir un compte de correu alié, encara que siga d'un treballador, es pot assemblar al registre d'una carta, escoltar les converses telefòniques o obrir la taquilla del treballador. Caldrà actuar per tant amb les mateixes consideracions, que solen resumir-se a obtenir una orde judicial, llevat que el tipus d'ús i les disposicions contractuals permeten una opció menys costosa en temps. Podem, això sí, comprovar si s'usa o no, durant quant de temps…, però no veure'n el contingut, en línies generals.

I els resultats mèdics? En les empreses es fan revisions anuals per a saber si el treballador és apte o no per a la faena que hi ha de fer, però els resultats són dades molt sensibles, amb una protecció especial.

D'altra banda, també hi ha dades que s'han de guardar un cert temps, per la qual cosa no es poden cancel·lar, però si limitar-ne l'ús.

Resta un altre tipus de dada singular: els sistemes de videovigilància. Les imatges són en si dades personals, per la qual cosa les consideracions que s'han de prendre han d'incloure, a més de les lògiques (no gravar converses ni llocs com ara vestidors o banys) totes les pertinents de protecció de dades.

El consentiment

Ens trobem possiblement davant d'un dels assumptes més espinosos, ja que es tracta d'un dels aspectes que més ha variat respecte a la legislació anterior. És imprescindible per al professional revisar l'article 7 del reglament.

Tot tractament de dades personals ha de ser lícit i lleial. Per a les persones físiques ha de quedar totalment clar que s'arrepleguen, s'utilitzen, consulten o tracten d'una altra manera dades personals que els concerneixen, així com la mesura en què es tracten o es tractaran. El principi de transparència, ho acabem de veure, exigeix que tota informació i comunicació relativa al tractament d'aquestes dades siga fàcilment accessible i fàcil d'entendre, i que s'utilitze un llenguatge senzill i clar. Aquest principi es refereix en particular a la informació dels interessats sobre la identitat del responsable del tractament i les finalitats que té i a la informació afegida per a garantir un tractament lleial i transparent respecte a les persones físiques afectades i al seu dret a obtenir confirmació i comunicació de les dades personals que els concernisquen que siguen objecte de tractament. 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 fer valdre els seus drets en relació amb el tractament.

En particular, les finalitats específiques del tractament de les dades personals han de ser explícites i legítimes, i s'han de determinar en el moment que s'arrepleguen. Les dades personals han de ser adequades, pertinents i limitades al que és necessari per a les finalitats per a les quals es tracten.

Per a poder considerar que el consentiment és «inequívoc», el reglament requereix que hi haja una declaració dels interessats o una acció positiva que indique l'acord de l'interessat. El consentiment no es pot deduir del silenci o de la inacció dels ciutadans.

El consentiment ha de ser verificable i que els qui recopilen dades personals han de ser capaços de demostrar que l'afectat els en va atorgar el consentiment.

S'exigeix de manera expressa que la informació que es proporcione siga fàcil d'entendre i s'ha de presentar en un llenguatge clar i concís.

Això requereix garantir que es limite a un mínim estricte el termini de conservació. Les dades personals només s'han de tractar si la finalitat del tractament no es poguera aconseguir raonablement mitjançant altres mitjans. Per a garantir que les dades personals no es conserven més temps del necessari, el responsable del tractament ha d'establir terminis per a suprimir-les o revisar-les periòdicament.

S'han de prendre totes les mesures raonables per a garantir que es rectifiquen o suprimisquen les dades personals que siguen inexactes. Les dades personals s'han de tractar d'una manera que garantisca una seguretat i confidencialitat adequades de les dades personals, inclusivament per a impedir l'accés o ús no autoritzats d'aquestes dades i de l'equip utilitzat en el tractament. (considerant 39)

Quan el tractament es du a terme amb el consentiment de l'interessat, el responsable del tractament ha de ser capaç de demostrar que l'interessat ha donat el consentiment a l'operació de tractament. En particular en el context d'una declaració per escrit feta sobre un altre assumpte, ha d'haver-hi garanties que l'interessat és conscient del fet que dona el consentiment i de la mesura en què ho fa. En tot cas, s'ha de tractar d'una formulació intel·ligible i de fàcil accés que utilitze un llenguatge clar i senzill, i que no continga clàusules abusives. Perquè el consentiment siga informat, l'interessat ha de conèixer com a mínim la identitat del responsable del tractament i les finalitats del tractament a les quals estan destinades les dades personals. El consentiment no s'ha de considerar prestat lliurement quan l'interessat no té verdadera o lliure elecció o no pot denegar o retirar el consentiment sense patir cap perjudici. (considerant 42)

El consentiment s'ha de donar mitjançant un acte afirmatiu clar que reflectisca una manifestació de voluntat lliure, específica, informada i inequívoca de l'interessat d'acceptar el tractament de dades de caràcter personal que el concerneixen, com una declaració per escrit, inclusivament per mitjans electrònics, o una declaració verbal. Això podria incloure marcar una casella d'un lloc web en internet, triar paràmetres tècnics per a la utilització de serveis de la societat de la informació, o qualsevol altra declaració o conducta que indique clarament en aquest context que l'interessat accepta la proposta de tractament de les seues dades personals.

El silenci, les caselles ja marcades o la inacció no han de constituir consentiment. El consentiment s'ha de donar per a totes les activitats de tractament fetes amb la mateixa o les mateixes finalitats. Quan el tractament tinga diverses finalitats, s'ha de donar el consentiment per a totes. Si el consentiment de l'interessat s'ha de donar arran d'una sol·licitud per mitjans electrònics, la sol·licitud ha de ser clara, concisa i no pertorbar innecessàriament l'ús del servei per al qual es presta. (considerant 42)[11]

Val la pena parar-se, si més no breument, per a subratllar les condicions per al consentiment.

1. Quan el tractament es base en el consentiment de l'interessat, el responsable ha de ser capaç de demostrar que l'interessat va consentir el tractament de les seues dades personals.
2. Si el consentiment de l'interessat es dona en el context d'una declaració escrita que també es referisca a altres assumptes, la sol·licitud de consentiment s'ha de presentar de manera que es distingisca clarament dels altres assumptes, de forma intel·ligible i d'accés fàcil i utilitzant un llenguatge clar i senzill. No és vinculant cap part de la declaració que constituïsca infracció del reglament. Un contraexemple pot ser el que hi ha quan en un banc se'ns pregunta si consentim que les nostres dades se cedisquen a filials seues i, si no hi donem el consentiment, se'ns «expulsa» del seu programa de punts de fidelització.
3. L'interessat té dret a retirar el consentiment en qualsevol moment. La retirada del consentiment no afecta la licitud del tractament basada en el consentiment previ a la retirada. Abans de donar el consentiment, se n'informa l'interessat. Serà tan fàcil retirar el consentiment com donar-lo.
4. En avaluar si el consentiment s'ha donat lliurement, s'ha de tenir en compte en la major mesura possible el fet de si, entre altres coses, l'execució d'un contracte, inclosa la prestació d'un servei, se supedita al consentiment al tractament de dades personals que no són necessàries per a l'execució d'aquest contracte.

Davant de qualsevol dubte, la recomanació immediata és consultar les directrius sobre el consentiment en el sentit del reglament (UE) 2016/679 (Grup de treball de protecció de les persones, grup de treball de l'article 29, 2018).

[11] No fa falta que al·ludim a contraexemples. El consentiment és, probablement, en la data en què s'escriu aquest text, el que pareix que els professionals han entès més malament. Cosa no gens estranya, encara que sí que resulta, si més no cridanera, que moltes webs d'ajuntaments seguisquen sense actualitzar els seus avisos legals i polítiques de privacitat i fent referència no ja a la LOPD, ometent al·lusions al reglament, sinó fins i tot a la LORTAD!, llei que es va derogar l'any 1999. Afortunadament, admeteu-me la ironia, ja no al·ludeixen a les «lleis i ordenances novament fetes per sa Majestat per a la governació de les Índies i bon tractament i conservació dels indis».
No obstant això, cal assenyalar un exemple no solament de desconeixement de la norma, sinó fins i tot de mala praxi claríssima: en almenys dos hospitals importants, gestionats per mans privades, he constatat que el consentiment es dona de manera implícita en firmar el registre d'entrada al servei, amb les caselles premarcades i al·ludint al fet que no acceptar-ne alguna implica canvis en el servei i sobretot en el pagament («En el cas d'oposar-se [...] serà íntegrament a càrrec seu [...] el pagament dels productes i/o serveis prestats»).

Usant dades d'altri. Usant dades en altres parts del globus

Sovint, el professional s'ha de fer càrrec d'unes dades de les quals no és el responsable del tractament, ni encarregat, ni tan sols membre de l'empresa on aquestes dades es gestionen. Pensem en una xicoteta gestoria que ha de fer els documents destinats a la seguretat social dels treballadors de les empreses clients. O pensem en una agència de viatges que intercanvia les dades dels clients amb la botiga de mobles que té davant, per a enviar-los publicitat. O filem més prim encara, i considerem que la nostra empresa té una sucursal a Mèxic i des d'allí se'ns demana una relació dels clients locals.

Al llarg del present epígraf intentarem desgranar els aspectes fonamentals d'aquest tipus de situacions, cada vegada més corrents.

Transferències de dades personals a països tercers (articles 44, 45, 46)

En la nostra societat globalitzada, on es produeixen diàriament intercanvis comercials entre ciutadans i empreses arreu del món, l'existència de fluxos transfronterers de dades personals és necessària per al dia a dia de persones, negocis i institucions. No obstant això, a mesura que s'incrementen els fluxos proporcionalment creix la inquietud sobre la possible reducció o desaparició de la protecció de les nostres dades de caràcter personal.

Per això, és precisa l'avaluació del tercer país, considerant de quina manera s'hi respecta l'accés a la justícia i com les normes que té són homologables a la legislació europea o no ho són. Cal adoptar decisions que, considerant la legislació vigent al país tercer, s'avalue si ofereix un nivell adequat de protecció equivalent en allò essencial al que s'ofereix respecte de les dades personals que són objecte de tractament, amb l'accent posat en si hi ha un control independent de la protecció de dades i en l'establiment de mecanismes de cooperació amb les autoritats de protecció de dades.

Si no hi ha una decisió que deixe clara l'adequació de la protecció de les dades, el responsable o l'encarregat del tractament llavors han de prendre mesures pel seu compte per a compensar la falta de protecció de dades al país tercer. Aquestes mesures poden passar per normes corporatives vinculants, o per clàusules tipus de protecció de dades (per exemple les que faciliten les autoritats de control).

Amb aquestes garanties s'han de garantir els drets exigibles i la possibilitat d'accedir a accions legals efectives, respectant no solament els principis generals relatius al tractament de les dades personals, sinó també els principis de la protecció de dades des del disseny i per defecte.

No podem oblidar que s'ha d'establir la possibilitat de mitjançar el consentiment explícit de l'interessat, i alhora la possibilitat de fer transferències quan així ho requerisquen raons importants d'interès públic.

Què ha de tenir en compte la comissió en avaluar l'adequació del nivell de protecció? A manera d'esquema:

1. L'existència d'un estat de dret, amb el respecte dels drets humans i les llibertats fonamentals, i la legislació pertinent.

2. L'existència d'autoritats de control independents al país tercer.

3. Els compromisos internacionals assumits pel país tercer o organització internacional.

Quan es determina que es té un nivell de protecció adequat, s'ha d'establir un mecanisme de revisió periòdica, almenys cada quatre anys. Si es determina que el país tercer o organització internacional ja no garanteix un nivell de protecció adequat, s'ha de derogar, modificar o suspendre, en la mesura necessària i sense efecte retroactiu la decisió.

La comissió ha de publicar en el Diari Oficial de la Unió Europea i en la pàgina web una llista de països tercers, territoris i sectors específics en un país tercer, i organitzacions internacionals respecte dels quals haja decidit que es garanteix, o ja no, un nivell de protecció adequat.

El responsable o l'encarregat del tractament només poden transmetre dades personals a un país tercer o organització internacional si ha oferit garanties adequades. Quines són les «garanties adequades»? Com es contrasten? Això es pot fer mitjançant:

1. un instrument jurídicament vinculant,

2. normes corporatives vinculants,

3. clàusules tipus de protecció de dades que adopta la comissió,

4. clàusules tipus de protecció de dades que adopta una autoritat de control i aprova la comissió,

5. un codi de conducta aprovat junt amb compromisos vinculants i exigibles del responsable o l'encarregat del tractament al país tercer,

6. un mecanisme de certificació aprovat, junt amb compromisos vinculants i exigibles del responsable o l'encarregat del tractament al país tercer d'aplicar garanties adequades.

Si hi ha autorització de l'autoritat de control, les garanties adequades es poden aportar mitjançant:

1. clàusules contractuals entre el responsable o l'encarregat i el responsable, encarregat o destinatari de les dades personals al país tercer o organització internacional, o

2. disposicions que s'incorporen en acords administratius entre les autoritats o organismes públics que incloguen drets efectius i exigibles per als interessats.

S'hi poden preveure una sèrie d'excepcions per a situacions específiques (article 47), de les quals destaquem les següents:

1. l'interessat ha donat explícitament el seu consentiment a la transferència proposada, després d'haver sigut informat dels possibles riscos;

2. la transferència és necessària per a l'execució d'un contracte o per a l'execució de mesures precontractuals adoptades a sol·licitud de l'interessat;

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

4. la transferència és necessària per a la formulació, l'exercici o la defensa de reclamacions o per a protegir els seus interessos vitals quan l'interessat estiga físicament o jurídicament incapacitat per a donar el consentiment;

Posem-ne un exemple, que és tota una categoria: els Estats Units. Els Estats Units òbviament no pertanyen a la Unió Europea, però els nostres continus fluxos comercials obliguen a fer que s'arribe a un enteniment en moltes coses. En la privacitat, que és el nostre cas, es va fer el 26 de juliol del 2000 en firmar un acord denominat «port segur» (*safe harbour*) pel qual les empreses estatunidenques que complisquen uns requisits bàsics passen a formar part d'un llista per la qual es permet la cessió de dades a aquestes empreses. La informació referent al cas es pot consultar en el web del Departament de Comerç dels Estats Units (The International Trade Administration, 2016).

El legislador òbviament és coneixedor que les grans tecnològiques dels Estats Units, alhora que ens subministren serveis, adquireixen un coneixement de nosaltres mateixos més gran que el que cada un de nosaltres puga tenir. Per això posa salvaguardes legals, sabent que s'intentaran saltar, perquè l'alternativa, tallar tota comunicació, és absolutament impensable.

Els propietaris de webs han de deixar clara la finalitat que té: si és una pàgina web privada per a amics o coneguts, o si no hi ha dades personals, no cal fer res. Però, i en el cas d'una associació, i si es tracta d'un club d'escalada? Llavors estarem sotmesos a la regulació de la privacitat. Igualment, si som autònoms, tindrem una sèrie de zones sensibles en la web, com el formulari de contacte, les dades dels clients que vulguen rebre les nostres novetats, l'enviament en si de correus electrònics, les *cookies* i fins i tot qui ha fet un «m'agrada» en la nostra pàgina de Facebook.

Cessió de dades i tractament de tercers

Si cerquem aquestes figures en el reglament, fent una cerca ràpida, veurem que no apareixen com a tals. No obstant això, en un context com el nostre, i amb el precedent de la LOPD de 1999, i la faena enorme desplegada sobre el tema des de fa molt de temps en arrere de l'Agència Espanyola de Protecció de Dades, convé dedicar un temps al tema, perquè es tracta de dues situacions quotidianes que poden suggerir confusió perquè a vegades no queden molt clares.

En la cessió de dades, l'organització a qui es cedeixen les dades ha de fer en tractament per si mateixa, mentre que en el tractament per tercers, és altri qui fa el tractament per a nosaltres.

En la cessió, el responsable del fitxer té obligació d'informar els afectats i indicar la finalitat del fitxer, la naturalesa de les dades i el nom i la direcció del cessionari. Sol incloure's una clàusula en la qual s'estableix que l'afectat accepta la cessió de les dades entre companyies del mateix grup i/o els seus agents comercials. No es considera comunicació de dades l'accés d'un tercer a la informació quan dit accés siga necessari per a la prestació d'un servei a l'empresa. La realització de tractaments per compte de tercers s'ha de regular en un contracte que ha de constar preferentment per escrit, i si no d'alguna manera que permeta acreditar-ne l'acord i contingut, i s'estableix expressament que l'encarregat del tractament únicament ha de tractar les dades d'acord amb les instruccions del responsable del tractament, la qual cosa implica que no les ha d'aplicar o utilitzar amb una finalitat diferent a la que figura en el contracte, ni les ha

de comunicar, ni tan sols per a la conservació, a altres persones. A més, ha de figurar en el contracte tota mesura de seguretat que l'encarregat del tractament està obligat a implementar.

D'altra banda, en el tractament per compte de tercers (per exemple contractem una gestoria perquè ens faça les gestions de la seguretat social amb dades dels nostres treballadors, o una empresa de màrqueting perquè envie publicitat als nostres clients) és imprescindible regular el transvasament de dades a través d'un contracte en el qual el tercer que accedeix a la informació es comprometa a garantir el compliment de la llei en els mateixos termes en què obliga al titular de les dades.

En tot cas, suposa un enviament de dades de caràcter personal a elements aliens a l'empresa, això és, una comunicació de dades personals, i per tant porta implícit que totes les parts implicades en la comunicació tinguen el deure de guardar secret sobre les citades dades. I pareix obvi, segons que pareix fins ara, que en enviar dades a tercers o permetre-hi l'accés, només podran ser usades per al compliment de finalitats directament relacionades amb les funcions legítimes del cedent i del cessionari amb el previ consentiment de l'interessat.

Recordem que hem parlat del consentiment. El consentiment per a la comunicació de les dades de caràcter personal a un tercer serà nul quan la informació que es facilite a l'interessat no siga clara en explicar la finalitat a què es destinaran les dades la comunicació de les quals s'autoritza, i/o el tipus d'activitat que fa aquell a qui es pretenen comunicar.

Recomanacions: és més que convenient estipular en el contracte de serveis amb el client les condicions i l'objecte per al qual es recapten les dades de caràcter personal així com la forma d'exercir els drets sobre aquestes dades.

Les *cookies*

No només fa falta recaptar el consentiment per al tractament de dades personals, sinó que també hi ha casos, com la instal·lació de les *cookies*, en què és obligatori.

Quan siga tècnicament possible i eficaç, el consentiment del destinatari per a acceptar el tractament de les dades es pot facilitar mitjançant l'ús dels paràmetres adequats del navegador o d'altres aplicacions, sempre que aquell haja de procedir a fer-ne la configuració durant la instal·lació o actualització mitjançant una acció expressa a l'efecte.

En tot, el responsable ha de recordar que quan la instal·lació i/o utilització d'una *cookie* comporte el tractament de dades personals, els responsables del tractament s'han d'assegurar del compliment de les exigències addicionals que estableix la normativa sobre protecció de dades personals, en particular en relació amb les dades especialment protegides. A més, és convenient recordar la necessitat d'adoptar cauteles addicionals en aquest àmbit en relació amb els menors d'edat.

«*Cookies* exceptuades» són les que tenen com a finalitat:

- *Cookies* d'«entrada de l'usuari»
- *Cookies* d'autenticació o identificació d'usuari (únicament de sessió)
- *Cookies* de seguretat de l'usuari
- *Cookies* de sessió de reproductor multimèdia

- *Cookies* de sessió per a equilibrar la càrrega
- *Cookies* de personalització de la interfície d'usuari
- *Cookies* de complement (*plug-in*) per a intercanviar continguts socials

La informació sobre les *cookies* facilitada en el moment de sol·licitar el consentiment ha de ser prou completa per a permetre els usuaris entendre la finalitat per a les quals s'instal·len i conèixer els usos que se'ls donaran.

Si s'ha d'obtenir el consentiment dels usuaris ja registrats per a instal·lar les *cookies* cal informar-los de manera verificable sobre els canvis fets en relació amb el tractament de les *cookies*.

Contractació de serveis *cloud computing*

És important identificar quins proveïdors de *cloud* estan localitzats dins de l'Espai Econòmic Europeu. Localització no només de la seu del proveïdor, sinó dels recursos físics. La contractació de serveis de *cloud computing* es fa a través d'un contracte de prestació de serveis que és imprescindible que vincule el compliment de la llei. Lamentablement, en la majoria dels casos, el que ofereixen els proveïdors són contractes amb clàusules contractuals tancades, sense opció per a negociar els termes.

El responsable ha de decidir per a quines dades personals contracta serveis de *cloud computing* i quines s'estima més mantenir en els sistemes d'informació propis. Aquesta decisió és important perquè delimitarà les finalitats per a les quals el proveïdor de *cloud* pot tractar les dades. El responsable ha de sol·licitar i obtenir informació sobre si intervenen o no terceres empreses (subcontractistes) en la prestació de serveis de *cloud computing*.

Perquè el responsable puga assegurar-se que les mesures de seguretat es compleixen, com a client ha de tenir l'opció de comprovar les mesures de seguretat, inclosos els registres que permeten conèixer qui ha accedit a les dades de les quals és responsable. El proveïdor de *cloud* ha d'informar diligentment el responsable, com a client, sobre les incidències de seguretat que afecten les dades de les quals el client és responsable, així com de les mesures adoptades per a resoldre-les o de les mesures que el client ha de prendre per a evitar els danys que puguen produir-se.

Normes que cal considerar:

- Llei de contractes del sector públic (RD legislatiu 3/2011, de 14 de novembre).
- Llei 11/2007 d'accés electrònics dels ciutadans als serveis públics, i RD 1671/2009 que desenvolupa parcialment aquesta llei.
- L'Esquema Nacional de Seguretat (ENS) i l'Esquema Nacional d'Interoperabilitat (ENI) (reials decrets 3/2010 i 4/2010, de 8 de gener).

Les autoritats de control: l'Agència Espanyola de Protecció de Dades

El considerant 117 ja anticipa que l'establiment d'una o més autoritats de control amb plena independència per Estat constitueix un element essencial de la protecció de les persones físiques pel que fa al tractament de dades de caràcter personal.

El fet que una autoritat de control puga o no actuar com a autoritat principal, segons que es tracten assumptes locals o quan afecta interessats d'aquest únic Estat membre provoca la coordinació necessària entre autoritats de control que ha d'informar sense dilació i decidir si s'ha d'emprar el «mecanisme de finestreta única»,[12] o si ho ha de tractar localment l'autoritat de control que n'haja informat. (considerant 127)

Recordem que en l'apartat de definicions dèiem que **autoritat de control** és l'autoritat pública independent que estableix un Estat membre conformement al que disposa l'article 51 del reglament. Convé que sapiem ara què diu l'article 51.

Cada Estat membre ha d'establir que siga responsabilitat d'una o diverses autoritats de control supervisar l'aplicació del reglament, per a protegir els drets i les llibertats fonamentals de les persones físiques pel que fa al tractament i de facilitar la lliure circulació de dades personals a la Unió. Autoritats de control que han de cooperar entre si. És possible que hi haja diverses autoritats de control en un Estat membre; una és la que represente aquestes autoritats en el Comitè (el Comitè és un organisme independent de la Unió amb personalitat jurídica, compost pel director d'una autoritat de control de cada Estat membre i el supervisor europeu de Protecció de Dades, o pels representants respectius).

Una vegada clar què és això d'una autoritat de control, en veurem uns quants aspectes d'interès. Comencem per la composició: qui són els membres de l'autoritat de control? (article 53)

Els membres de les autoritats de control han de ser anomenats mitjançant un procediment transparent, deixant que cada país de la Unió decidisca si ho seran mitjançant el Parlament, el Govern, el Cap d'Estat o un organisme independent encarregat del nomenament. En tot cas, cada membre ha de tenir la titulació, l'experiència i les aptituds, en l'àmbit de la protecció de dades personals, necessaris per al compliment de les funcions i l'exercici dels seus poders. És destituït abans d'acabar el mandat únicament en cas de conducta irregular greu o si deixa de complir les condicions exigides en l'acompliment de les seues funcions.
Cada Estat membre de la Unió ha d'establir referent als membres (article 54):

- les qualificacions i condicions d'idoneïtat necessàries per a ser nomenat membre;
- les normes i els procediments per al nomenament de membres de cada autoritat de control;
- la durada del mandat del membre o els membres de cada autoritat de control, no inferior a quatre anys, excepte el primer nomenament posterior al 24 de maig del 2016;
- el caràcter renovable o no del mandat del membre o els membres de cada autoritat de control i, si escau, el nombre de vegades que es pot renovar;
- les condicions, prohibicions relatives a accions, ocupacions i prestacions incompatibles amb el càrrec durant el mandat i després, i les normes que regeixen el cessament en l'ocupació.

[12] Serveix perquè els responsables que facen tractaments que afecten significativament ciutadans en diversos Estats de la UE tinguen una única autoritat de protecció de dades com a interlocutora. Això no suposa que els ciutadans s'hagen de relacionar amb diverses autoritats o amb autoritats diferents de la de l'Estat on residisquen. Sempre poden plantejar les reclamacions o denúncies a l'autoritat nacional pròpia.

L'autoritat de control que tenim a Espanya és l'Agència Espanyola de Protecció de Dades. És un ens de dret públic, amb personalitat jurídica pròpia i plena capacitat pública i privada. Actua amb plena independència de les administracions públiques en l'exercici de les seues funcions (cosa que no vol dir que siga totalment independent perquè està sotmesa al Tribunal de Comptes). Entra per tant en la categoria d'«administracions independents» excloses de la LOFAGE (Llei 6/1997, de 14 d'abril, d'organització i funcionament de l'Administració General de l'Estat).

La finalitat principal que té és vetlar pel compliment de la legislació sobre protecció de dades personals i controlar-ne l'aplicació. Per al compliment d'aquesta missió, l'Agència du a terme campanyes de divulgació per a una defensa més bona dels drets dels ciutadans. L'AEPD du a terme les seues potestats d'investigació fonamentalment a instàncies dels ciutadans, encara que també està facultada per a actuar d'ofici.

L'Agència Espanyola de Protecció de Dades (AEPD), creada en 1993, és l'organisme públic encarregat de vetlar que es complisca la Llei orgànica de protecció de dades de caràcter personal a Espanya. Té la seu a Madrid i l'àmbit d'actuació s'estén al conjunt d'Espanya.

A Espanya, a més, hi ha agències de protecció de dades de caràcter autonòmic a Catalunya i al País Basc, amb un àmbit d'actuació limitat als fitxers de titularitat pública que declaren les administracions autonòmiques i locals de les comunitats autònomes respectives.

Els membres i el personal de cada autoritat de control estan subjectes al deure de secret professional, tant durant el mandat com després.

Cal destacar (article 55) que les autoritats de control no són competents per a controlar les operacions de tractament dels tribunals en l'exercici de la funció judicial.

L'autoritat de control inclou en les competències pròpies (article 56): tractar unes reclamacions presentades o infraccions del reglament, i si s'està a la seu de l'establiment principal o de l'únic establiment del responsable o de l'encarregat del tractament de l'empresa que pretenga fer un tractament transfronterer de dades, actuar com a autoritat de control principal.

Unes quantes de les funcions que tenen (article 57)

De cara a l'interessat:

- amb sol·licitud prèvia, facilitar informació a qualsevol interessat en relació amb l'exercici dels seus drets;
- tractar les reclamacions presentades i investigar, en la mesura oportuna, el motiu de la reclamació i informar el reclamant sobre el curs i el resultat de la investigació en un termini raonable.

De cara a la societat en general:

- controlar l'aplicació del reglament i fer-lo aplicar;
- promoure la sensibilització del públic i la comprensió dels riscos, normes, garanties i drets en relació amb el tractament, amb una atenció especial als xiquets;
- assessorar el Parlament, el Govern i altres institucions;
- fer un seguiment de canvis que siguen d'interès, el desenvolupament de les tecnologies de la informació i la comunicació i les pràctiques comercials.

De cara al responsable i a l'encarregat del tractament:

- promoure la sensibilització dels responsables i encarregats del tractament sobre les obligacions que té;
- elaborar i mantenir una llista relativa al requisit de l'avaluació d'impacte relativa a la protecció de dades;
- oferir assessorament sobre les operacions de tractament;
- encoratjar l'elaboració de codis de conducta;
- fomentar la creació de mecanismes de certificació de la protecció de dades i de segells i marques de protecció de dades;
- elaborar i publicar els criteris per a l'acreditació d'organismes de supervisió dels codis de conducta;
- efectuar l'acreditació d'organismes de supervisió dels codis de conducta;
- autoritzar les clàusules contractuals i disposicions.

De cara a altres autoritats de control i funció investigadora:

- cooperar amb altres autoritats de control i prestar assistència mútua;
- dur a terme investigacions en particular basant-se en informació rebuda d'una altra autoritat de control o una altra autoritat pública.

Totes aquestes funcions han de ser gratuïtes per a l'interessat i per al delegat de protecció de dades, però quan siguen manifestament infundades o excessives, es pot establir una taxa raonable basada en els costos administratius o negar-se a actuar respecte de la sol·licitud. La càrrega de demostrar el caràcter manifestament infundat o excessiu de la sol·licitud recau en l'autoritat de control.

Poders de les agències de control (article 58)

De cara al responsable i a l'encarregat del tractament i, si escau, al representant del responsable o de l'encarregat, pot ordenar-los que faciliten qualsevol informació que requerisca per a l'acompliment de les seues funcions, així com obtenir del responsable i de l'encarregat del tractament l'accés a totes les dades personals i a tota la informació necessària per a l'exercici de les seues funcions, notificant al responsable o a l'encarregat del tractament les presumptes infraccions; per a fer-ho pot dur a terme investigacions en forma d'auditories de protecció de dades i revisar les certificacions expedides.

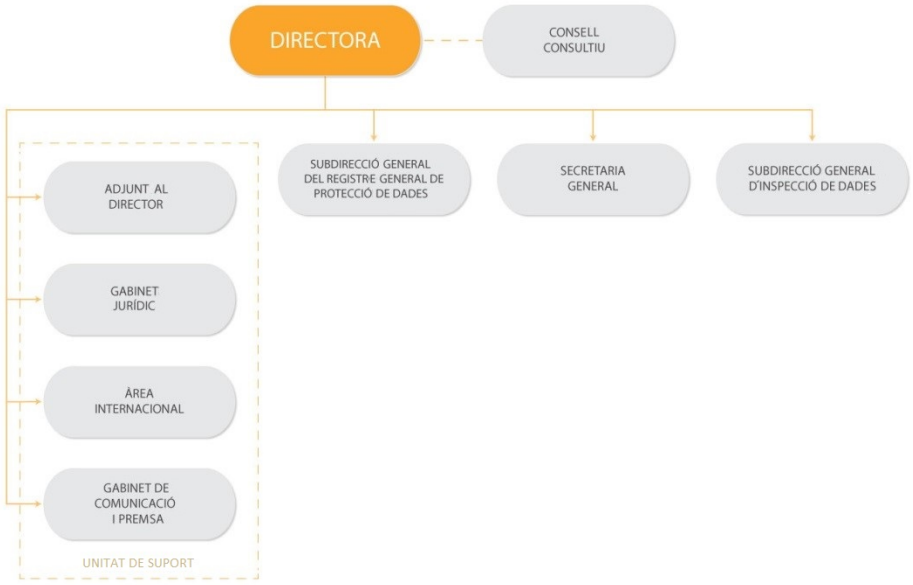
Una vegada es detecta alguna cosa sancionable, pot sancionar a tot responsable o encarregat del tractament amb un advertiment o amb una prevenció i ordenar al responsable o encarregat del tractament que atenguen les sol·licituds d'exercici dels drets de l'interessat, ordenant-los que les operacions de tractament s'ajusten a les disposicions del reglament, quan siga procedent, d'una manera determinada i dins d'un termini especificat; a més d'ordenar al responsable del tractament que comunique a l'interessat les violacions de la seguretat de les dades personals i ordenar la rectificació o supressió de dades personals o la limitació de tractament.

Pot imposar una limitació temporal o definitiva del tractament, inclosa la prohibició, retirar una certificació, imposar una multa administrativa i ordenar la suspensió dels fluxos de dades cap a un destinatari situat en un país tercer.

Des del punt de vista d'assessorament i informació, pot assessorar el responsable del tractament d'acord amb el procediment de consulta prèvia, emetre, per iniciativa pròpia o sol·licitud prèvia, dictàmens destinats al Parlament nacional, al Govern de l'Estat sobre qualsevol assumpte relacionat amb la protecció de les dades personals, emetre un dictamen i aprovar projectes de codis de conducta.

Agència Espanyola de Protecció de Dades

Encara que ja l'hem presentada, parlarem una mica de l'estructura que té i de com funciona. Comencem veient un organigrama de l'Agència Espanyola de Protecció de Dades:



Il·lustració 3. Organigrama de l'AEPD. Font: AEPD, 2018

Veiem dos elements molt singulars: el registre i la inspecció de dades. Els hi dedicarem unes línies, així com a la figura de la directora.

El registre general de protecció de dades:

Sense ànim exhaustiu, en aquesta part de l'AEPD:

Es promouen, registren i publiquen els codis de conducta, tramitant-los i valorant-ne les sol·licituds d'aprovació.

S'elaboren els criteris per a l'acreditació dels organismes de supervisió dels codis de conducta i es tramiten i se'n valora l'acreditació i revocació.

Es promouen els certificats, segells i marques en protecció de dades. S'elaboren els criteris per a l'acreditació dels organismes de certificació i se'n fa el control de les certificacions expedides i la revisió periòdica.

S'encarreguen d'elaborar i tramitar clàusules contractuals tipus de protecció de dades per a transferències internacionals.

Es tramiten i valoren les sol·licituds d'autorització de transferències internacionals de dades, i gestió de les comunicacions.

Es tramiten i valoren les sol·licituds d'aprovació de normes corporatives vinculants per a transferències internacionals de dades.

S'elaboren i tramiten les clàusules d'encarregats de tractament.

Dins de les campanyes de sensibilització de protecció de dades, destaquen les orientades a centres educatius i menors en particular, així com les orientades a pimes, les administracions públiques i les ONG.

S'elaboren materials d'ajuda a responsables i encarregats en el compliment de la normativa de protecció de dades.

S'atenen les consultes que plantegen responsables, encarregats i delegats de protecció. També s'atenen les consultes que presenten els ciutadans sobre exercici dels seus drets i presentació de reclamacions.

Es fa càrrec de les tares relatives a la transparència exigides a l'Agència.

Quan s'inscriu un fitxer es proporcionen les «característiques» del fitxer, no el fitxer en si. Per això, no és necessari renovar la inscripció si augmenten o disminueixen els particulars inscrits sinó quan canvien aquestes característiques (per exemple, es canvien les finalitats). A més, els fitxers públics s'han de publicitar en un diari oficial.

El registre de l'AEPD funciona amb silenci positiu. Si ha passat un mes des que es va enviar el fitxer i l'agència no ha dit res en contra, s'entén acceptat i registrat. El registre és gratuït i qualsevol persona pot fer-ho a través de la pàgina web de l'AEPD.

La inspecció de dades

De la mateixa manera, sense ànim de completesa, destaquem en les seues funcions la supervisió permanent del compliment de la normativa en matèria de protecció de dades per part dels responsables i encarregats dels tractaments, inclosa l'atenció als ciutadans en l'exercici dels drets que tenen d'accés, rectificació, oposició, supressió, oposició a decisions automatitzades, limitació al tractament i portabilitat. Per a fer aquesta supervisió al seu torn, s'analitzen les reclamacions per incidències concretes, per a determinar si les vulneracions de la normativa s'han produït per errors puntuals, o es deuen a causes sistèmiques, en aquest cas, l'Agència investiga l'origen del problema: això és, el sistema de gestió de dades del responsable o encarregat del tractament.

Es fan investigacions en forma d'auditories de protecció de dades, mantenint un diàleg permanent amb els delegats de Protecció de Dades, a l'efecte de resoldre les reclamacions que presenten els afectats.

Es comprova el compliment dels codis de conducta.

S'apliquen quan procedeix als poders correctius conferits a l'agència. Les seues actuacions d'inspecció s'orienten a aclarir els fets que presumptament puguen infringir la normativa en matèria de protecció de dades, la persona o òrgan que puga resultar responsable i la repercussió que puga haver-hi. Una de les seues manifestacions és l'exercici de la potestat sancionadora.

Altres labors: cooperar amb altres autoritats de control, proposar d'imposar una limitació temporal o definitiva del tractament, inclosa la prohibició, proposar d'ordenar la suspensió de fluxos de dades cap a un destinatari situat en un país tercer o cap a una organització internacional.

Poden examinar els suports d'informació i equips físics, requerir la documentació dels programes i fer auditories.

Directora de l'AEPD

La directora té la representació de l'agència i els actes que fa es consideren com a actes propis de l'agència. Les seues resolucions posen fi a la via administrativa i són recurribles a la sala contenciosa de l'Audiència Nacional. El nomenament l'efectua el Govern mitjançant Reial decret de qui compon el Consell Consultiu i a proposta del ministre de Justícia, amb un mandat de quatre anys. No pot rebre instruccions de cap poder o autoritat i actua amb plena submissió al dret. Exerceix les seues funcions amb dedicació exclusiva, plena independència i total objectivitat.

De les funcions que té, destaquem:

- Dictar les resolucions i instruccions que requerisca l'exercici de les funcions de l'Agència

- La coordinació amb les autoritats autonòmiques

- La representació de l'Agència en l'àmbit internacional

- Funcions de gestió (adjudicar i formalitzar els contractes; aprovar despeses i ordenar pagaments...)

Règim sancionador (articles del 77 al 84)

Al marge de la possibilitat d'exercir qualsevol acció judicial o recurs administratiu, l'interessat pot presentar una reclamació a una autoritat de control, la qual ha d'informar el reclamant sobre el curs i el resultat de la reclamació, sense oblidar informar sobre la possibilitat d'accedir a la tutela judicial. Es poden exercir accions contra una autoritat de control davant dels tribunals de l'Estat membre en què estiga establida.

En el cas d'una tutela judicial contra un responsable o encarregat del tractament, s'exerceix davant dels tribunals de l'Estat membre en el qual el responsable o encarregat tinga un

establiment. Però també es poden exercir en els tribunals de l'Estat membre on l'interessat té la residència habitual, llevat que el responsable o l'encarregat siga una autoritat pública d'un Estat membre que actue en exercici dels seus poders públics.

Tot aquell que patisca danys i perjudicis materials per una infracció del reglament té dret de rebre del responsable o l'encarregat del tractament una indemnització.

Qui respon dels danys? Qualsevol responsable que participe en l'operació de tractament ha de respondre dels danys i perjudicis causats en cas que l'operació no complisca el que disposa el present reglament. Un encarregat únicament ha de respondre dels danys i perjudicis que causa el tractament quan no haja complit les obligacions del reglament dirigides específicament a ell, o quan haja actuat al marge o en contra de les instruccions. Si demostren que no són responsables del fet que causa els danys, estan exempts de responsabilitat. Si el mal l'ocasionen diversos encarregats o responsables, cadascun se n'ha de responsabilitzar, a fi de garantir la indemnització. En aquests casos, si un responsable o encarregat del tractament paga una indemnització total pel perjudici ocasionat, té dret a reclamar a l'altra la part la indemnització corresponent.

Qualsevol infracció s'ha de castigar amb sancions, incloses multes administratives, amb caràcter addicional a mesures adequades que impose l'autoritat de control.

Si es tracta d'una infracció lleu, o si la multa que probablement s'imposava constituïra una càrrega desproporcionada per a una persona física, en lloc de sanció mitjançant multa es pot imposar una prevenció. La imposició de sancions, incloses les multes administratives, ha d'estar subjecta a garanties processals suficients. Els Estats membres tenen la possibilitat d'establir normes en matèria de sancions penals per infraccions del reglament. No obstant això, la imposició de sancions penals per infraccions d'aquestes normes nacionals i de sancions administratives no ha de comportar la vulneració del principi *ne bis in ídem* ('no dues vegades el mateix').

Les autoritats de control garanteixen que les multes administratives siguen en cada cas efectives, proporcionades i dissuasives. Per a determinar-ne la quantia s'ha de tenir en compte (entre altres):

1. La naturalesa, gravetat i durada de la infracció, tenint en compte la naturalesa, abast o propòsit de l'operació de tractament i el nombre d'interessats afectats i el nivell dels danys i perjudicis que hagen patit.
2. La intencionalitat o negligència en la infracció.
3. Mesures del responsable o encarregat del tractament per a pal·liar els danys i perjudicis.
4. Infraccions anteriors comeses.
5. Grau de cooperació amb l'autoritat de control amb la finalitat de posar remei i mitigar.
6. Les categories de les dades de caràcter personal afectades per la infracció.
7. Com l'autoritat de control en va tenir coneixement (el responsable o l'encarregat van notificar la infracció?).
8. L'adhesió a codis de conducta.

Es produeix un enduriment del règim sancionador, les sancions poden arribar fins als vint milions d'euros, o el 4% del volum de negoci total anual global de l'exercici financer anterior, la que siga

més alta. Per a la quantia de les multes administratives, s'aconsella consultar el reglament i la legislació estatal.

Mesures de seguretat

Important! Aquest apartat respon a una legislació no actualitzada encara a l'Estat espanyol: el Reglament de mesures de seguretat (BOE, 2008). Està en vigor mentre no contradiga al Reglament europeu de protecció de dades. Per la lentitud del legislador espanyol, s'incorpora a efecte informatiu, a falta d'una norma actualitzada.

El 25 de juny de 1999 es va publicar en el BOE el Reglament de mesures de seguretat (994/1999), relatiu als fitxers automatitzats que contenen dades de caràcter personal. Si bé va ser extensible durant diversos anys a qualsevol tipus de fitxer, el reglament l'ha substituït el Reial decret 1720/2007 de 21 de desembre, pel qual s'aprova (després de huit anys) el Reglament de desenvolupament de la LOPD. La publicació d'aquest reglament suposa un pas en ferm per part de l'administració espanyola per a completar la Llei amb un instrument tècnic que facilite la labor de l'Agència Espanyola de Protecció de Dades a l'hora de vetlar pel compliment de la legislació i controlar-ne l'aplicació.

El reglament de mesures de seguretat de fitxers amb dades personals (RMSDP) estableix tres nivells de protecció (alt –articles 101-104–, mitjà –articles 95-100– i bàsic –articles 89-94) i regula aspectes tan concrets com ara: documentació de seguretat reglamentària, gestió de suports, còpies de seguretat i recuperació, funcions i obligacions del personal, gestió i registre d'incidències, identificació i autenticació, control d'accés lògic, règim de treball fora de l'organització, fitxers temporals i control d'accés físic.

Les mesures de seguretat s'adopten segons els fitxers que manegem i suposen una «escala» en la qual, segons que augmenta la seguretat, els requisits del nivell inferior han d'estar coberts. Així, les dades que requerisquen el nivell alt han de cobrir així mateix les mesures dels nivells: bàsic i mitjà.

Nivell bàsic: qualsevol fitxer amb dades personals.

Nivell mitjà: fitxers de dades relatives a infraccions administratives o penals, Hisenda, serveis financers, solvència (fitxers de morosos), Seguretat Social, Mútues, de definició de la personalitat.

Nivell alt: fitxers de dades sobre ideologia, religió, creences, origen racial, salut, vida sexual o violència de gènere.

Nivell bàsic (articles 89-94) del RMSDP

S'han de complir les mesures de seguretat següents:

1. És necessari disposar d'un document de seguretat de l'organització, que en resumisca les actuacions quant a la protecció de dades. És un document intern que no és necessari donar d'alta en l'AEPD, però que, en cas d'inspecció, és obligatori presentar. Ha d'incloure les funcions i obligacions del personal que tracta les dades.
2. Les incidències previstes en un registre escrit.

3. Disposar d'un protocol per a controlar l'accés a les bases de dades.
4. Disposar d'una gestió controlada de suports i documents.
5. Disposar de mecanismes d'identificació i autenticació dels usuaris de les bases de dades, canviant-ne la contrasenya almenys una vegada a l'any.
6. Fer còpies de seguretat, com a mínim, setmanalment.

S'ha d'aplicar a qualsevol tipus de fitxer.

Nivell mitjà (articles 95-100) del RMSDP

Quant als fitxers de nivell mitjà, a més és obligatori:

1. Tenir un responsable de seguretat.
2. Fer una auditoria biennal (és a dir, cada dos anys).
3. Portar un registre d'entrada i eixida de dades.
4. Establir mesures addicionals per a la identificació i autenticació (per exemple, bloquejant l'accés després de tres intents fallits).
5. Controlar el lloc físic en el qual s'accedeix a les dades.
6. Disposar de sistemes de recuperació en cas d'incidències.

Nivell alt (articles 101-104) del RMSDP

Finalment, en els fitxers de nivell alt, a més de totes les mesures assenyalades s'han d'incloure:

1. Mesures de seguretat en la distribució de suports (per mitjà de claus i encriptació).
2. Tenir còpies de seguretat que estiguen a resguard d'incendis o algun tipus de sostracció (com per exemple guardades en caixes de seguretat).
3. Guardar els registres d'accés durant dos anys (o en algun cas durant més o menys temps).
4. Disposar d'encriptació de les telecomunicacions, especialment en xarxes públiques i sense fils, mitjançant sistemes d'encriptació.

Xicoteta taula-resum. Fitxers automatitzats

<table>
<tr><td rowspan="3">Nivell alt</td><td rowspan="2">Nivell mitjà</td><td>Nivell baix</td><td>Document de seguretat
Funcions i obligacions del personal
Registre d'incidències
Identificació i autenticació
Control d'accessos
Gestió de suports
Còpies de seguretat</td><td>Dades excloses dels nivells mitjà i alt
Nom
Cognoms
Direcció
Edat
Correu electrònic
Excepció article 81.5 del RDLOPD</td></tr>
<tr><td colspan="2">Control d'accés físic
Responsable de seguretat
Auditories biennals
Controls periòdics
Prova amb dades reals</td><td>Infraccions penals, administratives
Hisenda pública
Serveis financers
Perfil de l'individu
Impagats
Entitats gestores i serveis comuns de la Seguretat Social i responsables de mútues d'accidents de treball i malalties professionals de la Seguretat Social</td></tr>
<tr><td colspan="2">Xifratge de dades
Distribució de suports
Registre d'accessos
Telecomunicacions</td><td>Ideologia; religió; creences; vida sexual; salut; origen racial
Dades recaptades per a finalitats policials sense consentiment
Dades derivades de violència de gènere</td></tr>
</table>

		Operadors que presten serveis de comunicacions electròniques disponibles al públic o exploten xarxes públiques de comunicacions electròniques respecte a dades de trànsit i localització

Taula 2. Resum dels nivells de seguretat. Elaboració pròpia

Tractaments de dades amb peculiaritats

En aquest apartat anirem un pas més enllà. En l'anterior, acabàvem descrivint com hi havia una sèrie de dades que la legislació nacional protegia amb zel. Veurem com ho interpreta això el reglament, al mateix temps que veiem que ocorre amb elements peculiars, com ara les dades dels morts o les dels xiquets.

Categories especials de dades personals (article 9)

Hi ha una sèrie de tractaments prohibits: els que revelen l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques, o l'afiliació sindical, i el tractament de dades genètiques, dades biomètriques dirigides a identificar de manera unívoca una persona física, dades relatives a la salut o dades relatives a la vida sexual o les orientacions sexuals d'una persona física.

Veiem que es tracta d'elements que afecten la intimitat més profunda de l'individu. Així i tot, hi ha una sèrie d'excepcions. Aquestes dades es poden tractar si hi ha alguna de les circumstàncies següents:

1. Si l'interessat va donar el consentiment explícit per al tractament d'aquestes dades personals amb una o més de les finalitats especificades (si no hi ha una norma que ho impedisca).
2. Si el tractament és necessari per al compliment d'obligacions i l'exercici de drets específics del responsable del tractament o de l'interessat en l'àmbit del Dret laboral i de la seguretat i protecció social.
3. Si el tractament és necessari per a protegir interessos vitals de l'interessat o d'una altra persona física, si no està capacitat, físicament o jurídicament, per a donar-ne el consentiment.
4. Si el tractament l'efectua, en l'àmbit de les seues activitats, una fundació, una associació o qualsevol altre organisme sense ànim de lucre, la finalitat del qual siga política, filosòfica, religiosa o sindical.
5. Si el tractament es refereix a dades personals que l'interessat ha fet manifestament públiques.
6. Si el tractament és necessari per a la formulació, l'exercici o la defensa de reclamacions o per als tribunals.
7. Si el tractament és necessari per raons d'un interès públic essencial.
8. Si el tractament és necessari per a finalitats de medicina preventiva o laboral.
9. Si el tractament és necessari per raons d'interès públic en l'àmbit de la salut pública.
10. Si el tractament és necessari amb finalitats d'arxiu en interès públic, finalitats d'investigació científica o històrica o finalitats estadístiques.

Els Estats membres poden mantenir o introduir condicions addicionals, inclusivament limitacions, respecte al tractament de dades genètiques, dades biomètriques o dades relatives a la salut.

El tractament de categories especials de dades personals, sense el consentiment de l'interessat, pot ser necessari per raons d'interès públic en l'àmbit de la salut pública. «Salut pública» s'ha d'interpretar com tots els elements relacionats amb la salut, concretament l'estat de salut, amb inclusió de la morbiditat i la discapacitat, els determinants que influeixen en el dit estat de salut, les necessitats d'assistència sanitària, els recursos assignats a l'assistència sanitària, la posada a la disposició d'assistència sanitària i l'accés universal, així com les despeses i el finançament de l'assistència sanitària, i les causes de mortalitat. Aquest tractament de dades relatives a la salut per raons d'interès públic no ha de donar lloc al fet que tercers, com ara empresaris, companyies d'assegurances o entitats bancàries, tracten les dades personals amb altres finalitats. (considerant 54)

Xiquets (article 8)

Els xiquets mereixen una protecció específica, perquè són menys conscients dels riscos, conseqüències, garanties i drets concernents al tractament de dades personals. Això és d'una importància particular quan es tracta de l'ús de les seues dades amb finalitats de màrqueting o elaboració de perfils de personalitat o d'usuari. (considerant 38)

Si es fan ofertes directes a xiquets, el tractament de les dades personals d'un xiquet es considera lícit quan té com a mínim setze anys. Si el xiquet és menor, únicament és lícit si el consentiment el dona o l'autoritza el titular de la pàtria potestat o tutela sobre el xiquet. El límit de setze anys el poden rebaixar els Estats membres, però de manera que no siga mai inferior a tretze anys.

Considerem que a penes hi ha serveis que permeten saber l'edat d'algú. Això és així per com de complicada és la validació en poder enganyar amb facilitat: donant el DNI del pare, o amb accés a les comprovacions segures d'organismes públics i organitzacions autoritzades a compartir ordinador amb ells. Per a més informació sobre xiquets, xarxes socials i privacitat, es recomana consultar (De Miguel Molina, Oltra Gutiérrez, & Sarabdeen, An exploratory study on the privacy of children's images in Spain's most widely used social network sites (Tuenti and Facebook), 2010).

Condemnes i infraccions penals (article 10)

Només es pot fer sota la supervisió de les autoritats públiques, amb garanties adequades per als drets i llibertats dels interessats.

En el cas d'haver d'enfrontar-se a un supòsit d'aquestes característiques, és imprescindible revisar la Directiva (UE) 2016/680 del Parlament Europeu i del Consell de 27 d'abril del 2016, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les autoritats competents per a finalitats de prevenció, investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals, i a la lliure circulació d'aquestes dades i per la qual es deroga la Decisió Marc 2008/977/JAI del Consell (Directiva 2016/680 del Parlament Europeu i del Consell, de 27 d'abril del 2016, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les autoritats competents per a finalitats de prevenció, 2016).

Morts (considerants 27, 158 i 160)

El reglament no s'aplica a la protecció de dades personals de persones mortes, encara que els estats membres poden establir normes relatives sobre el tema. Cal considerar l'autorització per a establir el tractament ulterior de dades personals amb finalitats d'arxiu i amb finalitats d'investigació històrica, inclosa la investigació per a finalitats genealògiques, i per causes greus, com ara genocidi.

El Reglament de desenvolupament (BOE, 2008) sí que conté una previsió específica sobre el tema en l'article 2.4: «Aquest reglament no és aplicable a les dades referides a persones mortes. No obstant això, les persones vinculades al mort, per raons familiars o anàlogues, es poden dirigir als responsables dels fitxers o tractaments que continguen dades de la persona finada amb la finalitat de notificar-ne l'òbit, aportant-ne acreditació suficient, i sol·licitar, quan pertoque, la cancel·lació de les dades».

Tractament amb finalitats d'arxiu en interès públic, finalitats d'investigació científica o històrica o finalitats estadístiques (article 89)

S'han d'establir garanties de manera que es dispose de mesures tècniques i organitzatives, en particular per a garantir el respecte del principi de minimització de les dades personals. Parlem d'elements com la pseudonimització. Quan l'exercici dels drets derivats del tractament de dades personals amb finalitats d'investigació científica o històrica o estadístiques impossibiliten o obstaculitzen greument l'assoliment de les finalitats científiques, es poden establir excepcions.

El tractament de dades personals amb finalitats d'investigació científica s'ha d'interpretar de manera, inclòs el desenvolupament tecnològic i la demostració, la investigació fonamental, la investigació aplicada i la investigació finançada pel sector privat. Entre les finalitats d'investigació científica també s'han d'incloure els estudis fets en interès públic en l'àmbit de la salut pública. (considerant 159)

Per finalitats estadístiques s'entén qualsevol operació d'arreplega i tractament de dades personals necessàries per a enquestes estadístiques o per a la producció de resultats estadístics. Aquests resultats estadístics poden a més utilitzar-se amb diferents finalitats, incloses finalitats d'investigació científica. La finalitat estadística implica que el resultat del tractament amb finalitats estadístiques no siguen dades personals, sinó dades agregades, i que aquest resultat o les dades personals no s'utilitzen per a donar suport a mesures o decisions relatives a persones físiques concretes. (considerant 162)

Protecció de dades en esglésies i associacions religioses (article 91)

Ja sabem de dades que impliquen una intimitat molt especial. De les quals, les creences religioses i les idees polítiques figuren entre les destacades. Pel que fa al cas, les esglésies, associacions o comunitats religioses segons l'article estan subjectes al control d'una autoritat de control. Òbviament no se'ls pot impedir tot tractament, perquè llavors la gestió del dia a dia seria impossible.

Tractament i accés públic de documents oficials (article 86)

De nou ens trobem un altre cas de drets que se superposen. En aquest cas a privacitat enfrontem transparent. Com fer públic el que és privat? De quina manera una dada personal pot ser

transparent? Pel que fa al cas, el reglament indica que les dades personals de documents oficials en possessió d'alguna autoritat pública o un organisme públic o una entitat privada per a la realització d'una missió en interès públic les pot comunicar aquesta autoritat, organisme o entitat a fi de conciliar l'accés del públic a documents oficials amb el dret a la protecció de les dades personals.

Es té en compte el principi d'accés del públic als documents oficials, que és quelcom d'interès públic. S'ha de conciliar l'accés del públic a documents oficials i la reutilització de la informació del sector públic amb el dret a la protecció de les dades personals. Cal prestar una atenció particular als documents als quals no es pot accedir o amb un accés limitat en virtut de règims d'accés per motius de protecció de dades personals, i a parts de documents accessibles que continguen dades personals, la reutilització de les quals estiga establida com a incompatible amb el dret relatiu a la protecció de les persones físiques respecte al tractament de les dades personals. (considerant 154)

És interessant pel que fa al cas consultar la Directiva 2003/98/CE del Parlament Europeu i del Consell, de 17 de novembre del 2003, relativa a la reutilització de la informació del sector públic (DO L 345 de 31.12.2003, p. 90).

Altres dades especialment protegides (considerants 51 i 51)

Hi ha dades que, per la seua naturalesa, són particularment sensibles en relació amb els drets i les llibertats fonamentals, perquè el context del seu tractament podria comportar importants riscos: entre les quals hi ha les dades de caràcter personal que revelen l'origen racial o ètnic.

El tractament de fotografies no s'ha de considerar sistemàticament tractament de categories especials de dades personals, únicament es considerarien dades biomètriques quan el fet de ser tractades amb mitjans tècnics específics permeta la identificació o l'autenticació unívoques d'una persona física.

Aquestes dades personals no s'han de tractar, llevat que se'n permeta el tractament en situacions específiques. S'han d'establir de manera explícita excepcions, entre altres quan l'interessat done el consentiment explícit o si es tracta de necessitats específiques.

Altres excepcions: sempre que hi ha les garanties apropiades, en interès públic, en particular el tractament de dades personals en l'àmbit de la legislació laboral, la legislació sobre protecció social, incloses les pensions i amb finalitats de seguretat, supervisió i alerta sanitària, la prevenció o control de malalties transmissibles i altres amenaces greus per a la salut. També s'ha d'autoritzar a títol excepcional quan siga necessari per a la formulació, l'exercici o la defensa de reclamacions.

Breu aproximació ètica al tractament de dades

No pensem que per viure en un moment de màxima eclosió tecnològica reinventem normes ètiques i morals. Per a mostra, hi ha prou de fixar-nos en una frase d'un llibre de 1939!, que pareix escrit per a nosaltres ara mateix:

Una cosa és, almenys, claríssima: que les condicions de tot orde, socials, econòmiques, polítiques, en què treballarà demà són summament diferents de les que ha treballat fins ara.

No es parle, doncs, de la tècnica com de l'única cosa positiva, l'única realitat incommovible de l'home. Això és una estupidesa, i com més encegats estiguen per ella els tècnics, més probable és que la tècnica actual vaja a terra i periclite.

N'hi ha prou que canvie una mica substancialment el perfil de benestar que es veu davant l'home, que patisca una mutació d'algun calibre la idea de la vida, de la qual, des de la qual i per a la qual fa l'home tot el que fa, perquè la tècnica tradicional cruixa, es desllorigue i agarre altres rumbs. (Ortega y Gasset, 1968) (adaptació)

No, no hi ha res nou davall del sol. Però hi ha elements que produeixen interferències amb la nostra visió clàssica, de segles. Hobbes, en *Leviatan* (Hobbes, 2003), establia una cosa que havia acceptat tothom: el pacte de la ciutadania amb l'Estat per la seua seguretat. El pare Estat ha cedit el seu contracte a companyies com ara Movistar, Google o Facebook, que gestionen, quan no alguna cosa pitjor, les nostres dades i amb les dades la nostra seguretat, tant en la societat en xarxa com fora. I com és aquest contracte? Qui n'ha de vigilar les clàusules? Som conscients que ben sovint regalem les nostres dades als nostres proveïdors com Faust venia l'ànima al diable?

Dèiem que no inventem res. En efecte, ni tan sols des del camp de la informàtica. Des d'abans de l'eclosió d'internet l'assumpte ja preocupava. Per exemple, des de l'Institute of Electrical and Electronics Engineers (IEEE), una associació tremendament implicada en l'ètica de les TIC, en 1995 va aparèixer l'important en grandària i continguts *Ethics and Computing* (Bowyer, 1995), en què la privacitat ocupa un espai de molt d'interès, i amb una visió que podríem dir-ne actual: partint del que ell considera un precedent, les escoltes en línies telefòniques,[13] arriba al que denomina «Efecte Gran Germà», cercant la resposta en aquest moment únicament en la tecnologia, atès que la parca legislació estatunidenca poca resposta podia donar-li. En concret, se centra en l'encriptació, en la clau privada.[14] Pel que fa al cas, resulta interessant llegir, pel contrast, la sentència del Tribunal Suprem, sala penal, 1942/2016, en la qual s'avalen les escoltes amb mitjans tecnològics, inclosa la utilització dels telèfons mòbils i micròfons ambientals (Recurs de cassació per infracció de preceptes constitucionals i infracció de Llei, 2016). Sobre els estudis tècnics, destaquem (Landau *et al.*, 1994) i (Barlow, 1993). Sobre l'espionatge sistemàtic de l'Estat, (Oltra Gutiérrez, 2001).

D'una banda proclamem els drets humans, dels quals el dret a la intimitat de la persona, i de l'altra, amb les tècniques que ens són pròpies propiciem, si més no inconscientment, la vulneració d'aquest dret (pensem en fotografies aèries, satèl·lits, micròfons de mòbils, etc.). Ja no som sols un número per a un banc, un nom i cognoms substituïbles pel número del DNI. Som

[13] Des de 1928 es coneixen les intervencions de línies telefòniques per part de la policia per a lluitar contra el crim. Han evolucionat lentament, però constant. En 1968 es registren als Estats Units unes nou-centes escoltes legals de la policia. Poc després, el mateix concepte es trasllada a les converses via internet amb, per exemple, *sniffers* legals.

[14] Ha de fer-nos pensar això en per què les aplicacions que fan servir PGP, com a encriptació, tenen problemes transfronterers en considerar-los el legislador de l'altre costat de l'oceà com a armes.

tot el que té el fisc de nosaltres, tot allò relacionat al nostre permís de conduir, el nostre historial de la Seguretat Social… les vegades que hem consultat una cartellera de cinema, si hem vist un vídeo de Johnny Cash a través de Youtube, si ta mare consulta l'horòscop, si tens marques biològiques a la sang, el teu retrat antropològic… tot susceptible de ser codificat i de generar amb això espectres econòmics, sumant-los a informes teus que caminen dispersos, fins i tot antics com els antecedents patològics familiars, les dades de la teua gestació, fins i tot rumors sobre el teu caràcter. Som, en si, un gegantesc i voraç banc de dades on caben tots els fets i dits de la teua vida (Vázquez i Barroso, 1992).

Dia a dia, voluntàriament o involuntàriament, facilitem a grans bases de dades informació sobre els nostres desitjos, les nostres creences i ideologies, deixant un rastre viu dels restaurants on mengem, quin llibre comprem, amb qui parlem de manera suposadament privada amb aplicacions de missatgeria, quants diners tenim, per on hem passejat. Això ens porta ressons de Foucault (2012), l'efecte del panòptic, on fiquem un pres en una cel·la permanentment vigilada, assegurant així el funcionament automàtic del poder, perquè el presoner se sap contínuament observat. La conclusió òbvia, que la vigilància es pot considerar simultàniament deficient i excessiva, es pot aplicar als tractaments de dades sense control, pràcticament sense variar ni una coma. Amb una lectura directa, estem davant de la demanda creixent de seguretat i amb ella la necessitat de vigilància; i d'altra banda els efectes que aquesta vigilància té sobre la llibertat individual i col·lectiva. La qüestió de la privacitat queda llavors atrapada en un oxímoron que és «vigilar per a alliberar» (Colmenarejo Fernández, 2017).

Ací entra en joc el perfil del professional. Un professional de la informació té d'alguna manera un lloc d'àrbitre en aquest nou joc que es configura. Dit d'una altra manera, si desitgem viure en una societat justa, sense atropellaments, on les normes es respecten, lliure i on un poderós pel fet de ser-ho no «valga més» que un humil, necessitem bons professionals. Bons, en dos sentits: bons perquè es té un domini excel·lent de la tècnica i bons com a persones, que són capaces de mirar-se a l'espill sabedores que davant no tenen ningú que trenca l'ètica i la deontologia professional. Perquè si només som bons com a tècnics, menyspreant les normes de comportament, tirem al contenidor la part més important de la nostra humanitat i col·loquem falques per a trencar la nostra societat.

Òbviament, si plantejàrem en classe de forma oberta la pregunta «Què és una persona bona?», eixirien tantes respostes com alumnes. No, no hi ha, almenys soc incapaç de donar-la jo, una resposta única a la pregunta. Hi ha moltíssimes consideracions que s'hi han de tenir en compte. De fet, sobre aquestes matèries, els dubtes creixen. Com ens recorda López Calvo (2018), fins i tot en les persones amb formació tecnològica i jurídica sobre el tema, hi ha opinions divergents, fins i tot en l'àmbit judicial. Com la recent sentència del Tribunal Europeu de Drets Humans que condemna Espanya a indemnitzar cinc caixeres que robaven el seu ocupador per vulnerar el dret a la privacitat en ser gravades amb càmeres ocultes o l'habilitació de cessió a l'Agència Tributària per part d'Airbnb de les dades dels seus clients o pel Consell General del Poder Judicial de les dades d'advocats inclosos en Lexnet.

Ens plantegem una vegada i una altra debats vells com la humanitat. Aquesta combinació entre ètica, llei, decisions personals i decisions polítiques ens acompanyen des de l'antic Egipte, des dels codis primitius, en els quals ja s'al·ludeix a raons morals. En el cas de la privacitat, des de

l'article de Warren i Brandeis (1890) el lligen molts com un dret moral a ser protegit per la llei.[15] Per a organitzar una mica les idees, i seguint Colmenarejo Fernández (2017), enumerarem unes raons morals per a la protecció de les dades personals:

- Prevenció de danys. Per exemple, garantint que les contrasenyes d'accés són segures, o que la geolocalització no l'activen els dispositius sense consentiment de l'usuari.
- Evitar la desigualtat informativa. Les dades personals s'han convertit en mercaderies. Les persones solen estar en posició de desavantatge davant d'empreses o governs. Les lleis tenen com a objecte establir les condicions equitatives per a la redacció de contractes relatius a la transmissió i l'intercanvi de dades personals.
- Evitar la injustícia informativa, que pot comportar discriminació. La informació personal proporcionada en un context (per exemple durant una anàlisi mèdica) pot canviar el significat que té en un altre context (per exemple en processos de contractació o en transaccions comercials)[16] i desembocar en discriminació.
- No intromissió en l'autonomia moral. La falta de privacitat pot exposar els individus a forces externes que influeixen en les tries que fan. Pensem en les notícies falses que donen suport a un candidat davant d'un altre, que aconsegueixen ser les més difoses. Es mostren a més als usuaris que hi poden estar potencialment d'acord, fet que ens porta ecos del que anomenem «postveritat».

Recordem que el processament de dades exigeix que se n'especifique el propòsit, se'n limite l'ús, es notifique als individus i s'hi permet corregir inexactituds.

Hi solem trobar reticències. És habitual al·ludir a la neutralitat de les dades i de la tecnologia per a justificar la no necessitat de l'ètica en el que es denominen ciències empíriques. Les dades tenen una font, s'obtenen de persones o d'activitats que fan aquestes persones amb uns determinats mètodes i amb una o més finalitats. Això hauria de ser prou, per a alguns. El problema és que la grandària gran i el cada vegada nombre més gran provoquen canvis en les activitats relacionades amb la nostra identitat. La societat, a vegades de manera imperceptible, pateix canvis en la valoració del que és la privacitat, que comporta controlar dades d'altri i tan sols es desperta davant d'elements crítics com la necessitat gestionar la nostra reputació (Colmenarejo Fernández, 2017).

Podríem adduir una suposada objectivitat dels mètodes quantitatius. Suposada objectivitat que es fonamenta en la forma que tenen els sistemes d'informació d'eludir o evitar la intervenció humana. Això afermaria aquests paradigmes que ens parlen del determinisme tecnològic. Hem

[15] Podem pensar sense anar més lluny en la tan gastada per les pel·lícules de Hollywood quarta esmena, de 1789, text que aprovà definitivament Jefferson en 1792 com a part de la Carta de Drets redactats per a controlar els abusos governamentals als ciutadans després de la Guerra de la Independència, que diu així: «El dret dels habitants que ells i els domicilis, papers i efectes propis es troben a resguard de perquisicions i d'aprehensions arbitràries és inviolable, i no s'expediran a aquest efecte manaments que no es fonamenten en un motiu versemblant, estiguen corroborats mitjançant jurament o protesta i descriguen amb particularitat el lloc que s'ha de registrar i les persones o coses que s'han de detenir o embargar».

[16] Com es pot justificar la correlació de dades entre la informació d'un historial sanitari d'un ciutadà amb la informació sobre les cerques que fa en Google? Recordem webs com ara Patients like me, d'on es van robar dades per a vendre-les a companyies sanitàries. Això hauria de fer-nos reflexionar, entre altres coses, sobre la relació de l'exportació de dades amb la portabilitat com a nou dret de protecció de dades.

d'assumir que els atributs tècnics de la tecnologia s'han d'analitzar socialment i èticament, i no solament tècnicament, perquè les innovacions tecnològiques lluny de ser neutrals sempre estan orientades cap a una fi política (Colmenarejo Fernández, 2017). A més, hui, amb el «núvol», la dispersió de servidors al llarg del globus, que ens fa concebre les bases de dades com una cosa sense un entorn físic, ens provoca un distanciament extra en la qüestió moral. Ens recorda Colmenarejo una cita d'Aranguren, segons la qual davant d'un estímul els humans hem de conformar necessàriament la realitat abans de prendre una decisió, hem de parar-nos a pensar, parar-nos a justificar la nostra acció davant d'un ventall de possibilitats que se situa en la irrealitat. Diu Aranguren que la primera dimensió de la llibertat de les persones es dona precisament en el fet d'alliberar-se de l'estímul que suposa la reflexió. La segona dimensió de la llibertat que no s'és pròpia es fa efectiva quan prenem una decisió, quan decidim actuar d'una manera i no d'una altra, quan justifiquem els nostres actes hi ha la dimensió moral, que ens és inherent a tots els éssers humans, la nostra capacitat per a decidir-nos entre irrealitats possibles distingint entre bé, mal i allò que atén exclusivament els nostres interessos. I dit això: com conformem una realitat «no tangible»?

Pareix, per tant, que, d'una banda, la neutralitat de la tecnologia, que suposadament no té moral, i, de l'altra, la intangibilitat del bé a protegir, ens permet posar-nos de perfil. Cras error. Ens fonamentarem per a desmuntar-ho això en De la Cueva (2018). D'una banda, les solucions que donen els sistemes informàtics a unes necessitats de gestió de la informació no tenen cap suport jurídic, són meres interpretacions d'un humà, qui va construir l'algorisme. Això trenca en milanta trossos la idea de la neutralitat de la tecnologia. És més, ens converteixen en presos d'unes imposicions tècniques que no admeten discussió perquè es mostren com a irrebatibles, la qual cosa ens porta a una verdadera dictadura de la màquina. Ens queda pendent el, permeteu-me el joc de paraules, vaporós assumpte del núvol. Que no ho és tant, ja que no vegem les màquines, no significa que no existisquen i, per tant, queden lliures de subjeccions legals o morals.

No fa tant, se'ns deia que en Internet podíem passar pel que volguérem. Una *top model*, un camioner fort, un xiquet menut, un actor o un amant de les foques. Hui, això ha deixat de ser cert. Si som un amant de les foques, se sabrà. Se sabrà a més quines són les nostres foques favorites, en quin paral·lel es troben, com s'alimenten, quin seguiment en fem, quantes vegades hem anat a veure-les i que n'hem escrit. Inclús quina roba portàvem quan en vam escriure. Com es construeixen aquests registres? Quina transparència té el ciutadà d'aquests registres? Hi ha una sèrie de problemes sobre el tema que Colmenarejo Fernández (2017) enumera:

- Els usuaris no han arribat a comprendre com afecten aquestes violacions de privacitat tant d'individus com al comportament social d'aquests individus.
- Hi ha una falta de transparència quant a política de privacitat, la informació respecte de les anàlisis predictives.
- Dades falses. Resultats d'anàlisis falses es poden compartir a vegades de manera automàtica. Això dificulta que els usuaris puguen exercir el dret a corregir errors o falsedats que els afecten mitjançant un procediment adequat.
- Possibilitat de programar anàlisis que permeten predir amb exactitud de manera automàtica un rang d'atributs sensibles ampli com ara l'orientació sexual, creences religioses, ideologia política, ús de drogues, tests intel·ligència, etcètera.

- Desajust de les polítiques que reclamen els proveïdors, i els controls reals disponibles per a preservar la privacitat dels usuaris.
- Existència d'un incentiu policial similar per a usar tècniques avançades de vigilància.[17]
- Limitacions per a permetre l'anàlisi de dades privades, que fan que aquestes tècniques siguen vulnerables.
- Lleis de privacitat que es veuen ràpidament superades i que deixen d'ajustar-se a l'esperit de les lleis originals.

Plantegem-nos ara un altre dubte: si una persona cedeix intencionalment informació, quin dret tenen altres a fer aquesta informació pública? ¿La nostra mera existència és llavors un acte creatiu? Caldria parlar del dret a la propietat de les dades parlant de la lliure exposició d'aquestes dades per a fer-ne ús de la manera que considerem. El desafiament arriba en tractar el tema espinós de la publicitat actual, directa cap a nosaltres amb les dades que conscientment sovint els hem donat. Això és, potser cal protegir-nos de nosaltres mateixos, mitjançant tecnologia que està dissenyada amb requisits de privacitat en el programari i el maquinari. Per a fer-ho més còmode això, Colmenarejo Fernández (2017) proposa una taxonomia de la privacitat d'acord amb els diferents moments:

1. Arreplega: vigilància i interrogació a fi de captar dades.
2. Procés: recopilació, identificació, seguretat, ús secundari i exclusió.
3. Difusió: violacions de confidencialitat, revelació, exposició indeguda, facilitat d'accés, xantatge, apropiació i distorsió.
4. Intrusió i interferència en la presa de decisions.

Què caracteritza hui l'ús de les bases de dades? Segons Colmenarejo Fernández (2017), es pot resumir en «les cinc V»: volum, velocitat, varietat, veracitat i valor.

Codis de conducta (articles del 40 al 42)

Acabem de veure com, en tota actuació professional, no només s'ha de complir la llei. La llei és el que ens controla des de fora, però hi ha un control superior que és l'interior. Pel que fa al món de la protecció de dades, amb una necessària proactivitat dels responsables, l'existència d'uns codis que ajuden a delimitar unes vies adequades es converteix en quelcom, més que important, quasi imprescindible. Així, el reglament incita a associacions que representen responsables o encarregats a fer que elaboren codis de conducta,[18] amb la finalitat de facilitar-ne l'aplicació

[17] És d'interès visualitzar el documental *Pre-Crimen* (Hielscher i Heeder, 2018).

[18] Podem enllaçar això amb els criteris per a la construcció de codis deontològics o de bona pràctica professional, en els quals ha de figurar (Garriga Domínguez, 2010):
• Condicions d'organització
• Règim de funcionament
• Procediments aplicables
• Normes de seguretat dels fitxers
• Obligacions dels responsables del fitxer i de les altres persones que intervinguen en el tractament o ús de dades personals.
• Les garanties per a l'exercici dels drets de les persones afectades.

efectiva, interpretant les característiques específiques en cada sector i les necessitats específiques, sobretot, de les pimes.

En aquests codis és interessant establir les obligacions dels responsables i encarregats.

Per a elaborar-los, o modificar-los si escau, cal consultar les parts interessades.

Elements que s'han de considerar en aquests codis:

1. el tractament lleial i transparent,
2. els interessos legítims que persegueixen els responsables,
3. l'arreplega de dades personals,
4. la pseudonimització de dades personals,
5. la informació proporcionada al públic i als interessats,
6. l'exercici dels drets dels interessats,
7. la informació proporcionada als xiquets i la protecció dels xiquets,
8. la notificació de violacions de la seguretat de les dades personals,
9. la transferència de dades personals a països tercers.

Les associacions i altres organismes que projecten elaborar un codi de conducta o modificar o ampliar un codi existent han de presentar el projecte de codi o la modificació o ampliació a l'autoritat de control competent. Si el projecte de codi o la modificació o ampliació s'aprova, l'autoritat de control registra el codi i el publica. El Comitè arxiva en un registre tots els codis de conducta, modificacions i ampliacions que s'aproven, i els posa a disposició pública per qualsevol mitjà apropiat.

Certificació

Es promou la creació de mecanismes de certificació en matèria de protecció de dades i de segells i marques de protecció de dades a fi de demostrar el compliment del que es disposa en el present reglament en les operacions de tractament dels responsables i els encarregats.

Aquests mecanismes de certificació, segells o marques de protecció de dades tenen l'objecte de demostrar l'existència de garanties adequades que ofereixen els responsables o encarregats no subjectes al present reglament. Aquesta certificació és voluntària i ha d'estar disponible a través d'un procés transparent. S'expedeix a un responsable o encarregat de tractament per un període màxim de tres anys i es pot renovar en les mateixes condicions, sempre que es continuen complint els requisits pertinents. La certificació es retira quan no es complisquen o s'hagen deixat de complir els requisits per a la certificació.

El Comitè arxiva en un registre tots els mecanismes de certificació i segells i marques de protecció de dades i els posa a disposició pública per qualsevol mitjà apropiat.

Els organismes de certificació els ha d'acreditar l'autoritat de control, l'organisme nacional d'acreditació (Reglament (CE) núm. 765/2008 del Parlament Europeu i del Consell d'acord amb la norma EN ISO/IEC 17065/2012), o tots dos. Aquesta acreditació s'expedeix per un període màxim de cinc anys i es pot renovar en les mateixes condicions.

Situació i conclusions

L'ésser humà pareix que deixa de ser sobirà per a passar a ser un flux de dades en una unitat controlada. Mentre les empreses privades creixen en poder no només econòmic, sinó també polític i social, com podem veure pels missatges dominants que ens envolten… o per les possibilitats de guanyar eleccions usant les xarxes socials…

Està en mans del professional conduir aquesta situació a bon terme, però… les notícies que ens envolten porten a una gran confusió. Llegim en la premsa dades sorprenents i titulars encara més cridaners (per exemple «España alerta de las asesorías "a coste cero": "Son una estafa para empresas"», en *El economista*, el 26 d'abril del 2018).

Efectivament, les empreses pareix que es dividisquen entre les que s'han assabentat que hi ha una legislació europea de protecció de dades i intenten fer alguna cosa, amb èxit divers, i les que encara «passen», per no parlar de casos pitjors (recordem l'assumpte de Cambridge Analytica amb les dades preses de Facebook).

S'ha de tenir en compte la dificultat d'harmonitzar en una legislació les vint-i-set precedents dels diferents països de la Unió, alhora que s'ha de vigilar que els canvis produïts per la legislació es duguen a terme de manera raonable. Tots han rebut una pluja de peticions de consentiment que, al mateix temps que ens recorda la nostra vida digital i tants anys de regalar les nostres dades per internet, ens fan veure que entrem en una nova era.

La dificultat ens la pot mostrar l'enquesta conjunta d'IDC i Microsoft, sobre «Com accelerar el compliment del GDPR» (IDC, 2018). Segons l'informe, amb base de cent empreses de 250 treballadors, a punt d'entrar en vigor el reglament, un 65% de les empreses deien que no podien garantir els canvis precisos, davant del parc 10% que ja els havien fet i un 25% amb plans en curs.

Aquesta realitat podem contrastar-la amb les memòries de l'AEPD. En concret, en la memòria del 2017 podem trobar les dades següents:

- Denúncies rebudes sobre el tractament de dades en Internet: 762 en el 2017 enfront de 557 en el 2015
- Reclamacions per tutela de drets:
    - 744 per cancel·lació o supressió
    - 376 per accés
    - 37 per rectificació
    - 51 per oposició
- Total de consultes efectuades: 256.000

És, de nou, el professional la peça clau perquè aquest complicat mecanisme de rellotgeria no endarrerisca, no avance… i no es pare.

Aspectes que hem vist que poden tamisar la nova LOPD (Congrés dels Diputats, 2017), en fase final de tramitació en el moment de la redacció d'aquestes línies. Per exemple, sobre el tema espinós dels difunts, hi ha un règim jurídic per a hereus: l'article 3 del projecte de llei ens diu que els hereus es poden dirigir a responsable de tractament, excepte si el finat no va dir una

altra cosa o hi ha una llei que ho impedisca. També apareixen canvis pel que fa als menors (menors, els tutors o el Ministeri Fiscal; el mateix per a discapacitats menors) on es rebaixa l'edat crítica de catorze a tretze anys.

Aquest tipus de legislació és susceptible de rebre molts canvis, per la promulgació de noves lleis, directives…, o per la correcció de les actuals (per exemple, Europea, 2018). Aquests canvis s'actualitzen mitjançant annexos al present tema, en el lapse entre l'aparició i la correcció.

Un exemple de pròxima actualització el tenim en la «e-privacy» (Comissió Europea, 2017). Encara en procés, aquest futur reglament se centra especialment en les comunicacions digitals i els paràmetres de compatibilitat entre privacitat i economia digital, ha de regular aspectes com la protecció de la privacitat en determinats serveis en línia o en les dades dels navegadors. Actualment s'aplica una directiva de l'any 2002, com es pot entendre, obsoleta en molts aspectes, per això des del 2009 es fan passos per a substituir-la, aquesta vegada com a reglament, per a evitar problemes a l'hora d'execució simultània en els diferents països de la Unió. Un dels aspectes que s'hi han de renovar és la millora dels navegadors pel que fa a la protecció de dades, perquè ha de deixar d'importar el dispositiu que s'utilitze. És un tema que entra en l'anomenada privacitat per disseny i que cerca que els usuaris no hagen de visitar innombrables i canviants menús per a protegir les seues dades. També apareixen regles estrictes per a les *cookies*.

Eines d'utilitat

Per a finalitzar, donem una sèrie de pistes sobre eines per a localitzar legislació i normes.

La principal és la pàgina del BOE, on podem trobar la legislació actualitzada, alhora que disponible en compendis («codis»): <www.boe.es>.

Per a la legislació de la Unió, hi ha un cercador similar, multiidioma: <https://eur-lex.europa.eu/homepage.html?locale=es>.

Autenticats en la xarxa de la UPV i des de dins, podrem accedir als cercadors d'AENOR, per a normes tècniques i ARANZADI, del qual se'n destaca l'arxiu de jurisprudència.

Altres normes d'interès:

A més de les ressenyades en el tema, cal destacar:

- Directrius sobre el consentiment en el sentit del Reglament (UE) 2016/679 (Grup de treball de l'article 29 sobre protecció de dades, 2017)
- Orientacions de la Comissió sobre l'aplicació directa del Reglament general de protecció de dades (Comissió Europea, 2018)
- Per a desenvolupadors d'aplicacions mòbils, hi ha un document del grup 29 imprescindible (Article 29 Data Protection Working Party, 2013)
- Reglament (CE) núm. 765/2008 del Parlament Europeu i del Consell, de 9 de juliol del 2008, pel qual s'estableixen els requisits d'acreditació i vigilància del mercat relatius a la comercialització dels productes i pel qual es deroga el Reglament (CEE) núm. 339/93 (Parlament Europeu i Consell de la Unió, 2008)
- Requisits per a organismes que certifiquen productes, processos o serveis (AENOR,

2012)

Altres textos d'interès:

Per a aprofundir en determinats temes:

- AGPD: Procedimiento por incorporación a un grupo de Whatsapp (AEPD, 2017)
- AGPD: Procedimiento por transmisión de fotos por Whatsapp (AEPD, 2017)
- AGPD: Procedimiento sancionador contra Google Street View (AEPD, 2017)
- Circular del ministeri fiscal sobre intervenció de comunicacions electròniques (Fiscalia General de l'Estat, 2013)
- *Derecho al olvido. Caso Mario Costejá* (Google vs Mario Costejá, 2014)
- La cort d'apel·lació dels Estats Units declara que els «m'agrada» de Facebook els protegeix la primera esmena (Bland vs Roberts, 2013)
- *Libertad de información, derecho a la propia imagen y autocensura de los medios* (Salvador, Rubí, Ramírez, 2011)
- *Menores en internet* (Davara Fernández de Marcos, Madrid)
- Sentència «Derecho al olvido digital. Digitalización de hemeroteca sin utilizar códigos ni instrucciones que...» (2015)
- Sobre l'ús de càmera oculta: la tesi doctoral de Gómez Sáez (2014)
- Sobre tractament de les dades sanitàries: Medinacelli Díaz, 2016

Preguntes de tipus test. Exemples

El Reglament europeu de protecció de dades s'aplica a...

a) les persones jurídiques.
b) les persones físiques.
c) *a)* i *b)* són correctes.
d) la inscripció en el Registre general.

Resposta correcta: *a)*. Pàgina 2.

Pertinència és sinònim de:

a) Veracitat.
b) Seguretat.
c) Lleialtat.
d) Cap de les anteriors.

Resposta correcta: *d)*. Pàgina 11.

Els moments del tractament de protecció de dades són:

a) Cessió, tractament i utilització
b) Arreplega, dissociació i utilització
c) Arreplega, tractament i utilització

d) Arreplega, tractament i portabilitat

Resposta correcta: *c)*. Pàgina 14

L'interessat té dret a obtenir sense dilació indeguda del responsable del tractament...

a) la rectificació de les dades personals inexactes que el concernisquen.
b) la dissociació de les dades personals inexactes que el concernisquen.
c) la dissociació de les dades personals exactes que el concernisquen.
d) Totes les respostes anteriors són correctes.

Resposta correcta: *c)*. Pàgina 19

Fa falta un lleuger de protecció de dades...

a) si es tracta d'un tractament des de l'administració pública.
b) quan es treballa amb dades d'un nombre elevat de persones.
c) quan es treballa amb un nombre elevat de dades especials.
d) Totes les respostes anteriors són correctes.

Resposta correcta: d). Pàgina 25.

Cas. El mort pixelat

Història de quasi ficció, inspirada en fets reals, però allunyada de personatges identificables de qualsevol manera. Qualsevol truculència o frase fora del test es deu únicament a la meua esbojarrada imaginació i, per descomptat, no es correspon gens ni mica amb la realitat. Si algun protagonista comet alguna malesa o manté actituds reprovables, atribuïu-ho a l'ànim de fer més digerible el text. En tot cas, senyoria: animus jocandi*!*

Alcahuete de las Fuentes és un poble tranquil. Pels carrers s'hi respira la pau tot l'any, llevat del mes d'agost, en què les veus dels xiquets tornen a retronar-hi, i el ball destrossa cançons de Johnny Cash per honorar el patró.

El lloc més habitat del poble és el cementeri. I és que la terra estira, diuen que. I per això els nascuts al poble, encara que desertaren de l'aladre fa dècades per anar a viure a les ciutats, volien que els seus ossos reposaren eternament en el seu estimat Alcahuete de las Fuentes.

Aquest va ser el cas de Tiburcio. El tio Tiburcio va deixar el poble amb vint anys, novença, i ell i la dona es van instal·lar en una pedania de Valencianemburg. Va treballar en una fàbrica de cervesa fins que es jubilà i, quan va morir, Maruja, la viuda, va complir el seu darrer desig: el va enterrar al cementeri del poble.

Maruja va complir la inveterada tradició que porta les dones a sobreviure algun lustre el marit i així, envoltada de nebodes i de gats, perquè de fills no en van tindre, trenta anys després va notar com la Parca li amerava el cor trencat tres dècades abans. Va llegar els béns (un pis de tres habitacions, on va viure des que van arribar del poble, i un apartament a la platja, amb més rovell als metalls que el casc del *Titanic*) a la seua neboda Adalberta, amb la condició que l'enterraren amb el seu estimat Tiburcio.

Tita (d'Adalberta, Adalbertita, i d'Adabertita, Tita, que queda molt *guai*), amb una mica d'angúnia, que tot cal dir-ho, se'n va fer càrrec. Bé, en realitat vull dir que va carregar quasi literalment el mort, la morta en aquest cas, al seu estimat Petronilo, Petro, el seu espòs, a qui va conèixer en una convenció de gent amb noms estranys i amb odi etern cap als pares.

Petro va preparar els papers, va regalar els gats, va gestionar l'herència i, amb la morta a bord de la carmanyola amb rodes corresponent, va acompanyar Tita a l'enterrament de la seua estimada tia.

Una vegada a Alcahuete de las Fuentes, van arribar al cementeri. El senyor Pancracio Bovedillas, l'enterrador, els hi esperava. Ell i el senyor rector eren els únics de tot el poble que hi van acudir. Cosa lògica d'altra banda, perquè dels altres 218 habitants del poble, ningú recordava aquella bona dona que havia eixit d'allà tants anys arrere.

Com que Tita era atea militant, demanà al sacerdot, amb una amabilitat gèlida com un frigorífic de doble cos, que se n'anara cap a la seua església. I com que el *pater* no era difícil de convèncer en aquest aspecte, se n'anà a passeig i els deixà sols a tots quatre: Tita, Petro, Pancracio i el cadàver. Pancracio va pensar que amb una sessió d'espiritisme, hi havia allà la gent justeta per a una partida de pòquer, però de seguida va oblidar aquests pensaments quan va topar de cara amb l'inesperat.

Tiburcio estava incorrupte! El cos de Tiburcio, momificat, pareixia que els saludava, en obrir la caixa. Només li faltava el *Marca* o l'*As* davall del braç per a ser igual que un dels parroquians de la plaça del poble.

«Què faig?», va pensar. «La xicona aquesta de la ciutat pot ser que se'm desmaie quan li diga que son tio està esperant-la ací, de cos present». Però no va poder pensar-hi molt de temps. Quan va veure que Pancracio no apartava els ossos de l'oncle per ficar al taüt el nou cadàver, Petro s'hi va acostar i va veure el panorama. Va amollar un crit:

«Tita! Mira, tenim una mòmia en la família! Escolte, amic, pose'l a terra, que em gitaré al costat d'ell i farem unes fotos per al *feisbus*».

Pancracio es va quedar lívid quan va sentir el clic de la foto del mòbil. Ai, tan bé que estaria fent un rebentat a la plaça…

oOo

Va passar el temps, i l'alcalde president el va cridar al despatx. Cosa normal, estava acostumat que li demanaren informes, i l'alcalde era un d'aquests individus presumptuosos, que pareixia que es pensava que, en comptes de manar en un poble de 200 ànimes, era el ministre de la guerra d'un gran imperi del segle XIX. Foto del rei tapant un clevill, bandera del municipi i l'autonòmica tapant-ne un altre… foto del líder polític de torn (no tenia manies en qüestió de partits, mentre el mantingueren en el càrrec)… en fi, l'habitual.

Però aquesta vegada… ah… aquesta vegada l'alcalde no estava sol. Dos advocats l'acompanyaven. Damunt la taula, diversos periòdics amb una foto en portada: la seua, amb el

tio Tiburcio al costat. La perspectiva feia l'efecte que l'abraçara per a fer-hi un pas de ball. Pancracio va envellir deu anys de colp en veure-ho.

Estava a punt de caure-li'n una de ben grossa. Els nebodets havien estès pertot arreu la sessió fotogràfica. L'alcalde el va avisar que alguna sanció li cauria, però que primer havia d'emetre un comunicat lamentant el fet.

Llavors, un petit receptor de televisió treia la imatge de la discòrdia. Van apujar la veu. Van aparèixer en carrusel les imatges de la sessió, amb una cara pixelada: la del difunt. Tita, Petro i Pancracio hi apareixien a cara descoberta, encantats d'haver-se conegut. Van apujar la veu. Tita es disculpava, deia que era una foto feta per al seu grup familiar proper, que no podia imaginar que apareguera a la portada de l'*Heraldo* de Mèxic el mateix dia. Demanava perdó a qui haguera pogut ofendre, la veu la tenia molt compungida.

Llavors el locutor va començar a dir que la policia judicial investigava l'assumpte, i a recitar l'article 526 que es refereix a «la falta al respecte deguda a la memòria dels morts, violar els sepulcres o sepultures, profanar un cadàver o les cendres...» i que preveu penes de presó de tres a cinc mesos i sancions econòmiques. Un delicte d'ofensa als difunts, en tota regla.

Elements per al debat

1. Veiem que es produeix un pixelació de rostres. En aquest cas, només del mort, no dels vius.
2. Pancracio mostra una actitud passiva de Pancraci, és víctima o còmplice?
3. Protecció de dades i cadàvers és una mescla que sol confondre, de quina norma parlem?
4. No hi ha terceres persones que hagen fet ús d'aquestes fotos. Fins que la premsa les col·loca enmig de tot, i es produeix l'explosió. És lògica la censura hui? Recordem casos precedents. Retirada d'una edició d'*El Jueves*, per exemple.
5. Hi ha molts personatges desfilant, en primer o segon pla: treballador municipal, responsable polític, familiars directes, periodistes que difonen fotos sense pixelar o pixelades, *retwittejadors* anònims… fins a on arriben les diferents responsabilitats?

Notícies reals que van inspirar de manera remota aquesta ficció, sens dubte totalment allunyada de la font primigènia:

(Consultades el 2 de juliol del 2018)

- http://www.diarioinformacion.com/vega-baja/2014/09/12/sobrina-hizo-foto-cadaver-tio/1544440.html
- http://www.diarioinformacion.com/vega-baja/2014/09/11/ayuntamiento-aparta-enterrador-mantener-pie/1543904.html
- http://www.diarioinformacion.com/vega-baja/2014/09/11/investigan-delito-ofensa-difuntos/1543903.html

Bibliografia

AENOR. *Avaluación de la Conformidad. UNE-EN ISO/IEC 17065*. Madrid: AENOR, desembre del 2012.

AGÈNCIA ESPANYOLA DE PROTECCIÓ DE DADES. (2017). *Denuncia del Ayuntamiento de La Font de la Figuera. PS/00576/2017*. Madrid: AEPD, 2017.

AGÈNCIA ESPANYOLA DE PROTECCIÓ DE DADES. 26 de maig del 2018, recuperat el 18 de juliol del 2018, de: https://www.aepd.es/

AGÈNCIA ESPANYOLA DE PROTECCIÓ DE DADES. *Google Street View. Procedimiento Nº PS/00541/2010*. Madrid: AEPD, 2017.

AGÈNCIA ESPANYOLA DE PROTECCIÓ DE DADES. *Infracción de Administraciones Públicas instruido por la Agencia Española de Protección de Datos al Ayuntamiento de Boecillo. Procedimiento Nº AP/00023/2017*. Madrid: AEPD, 2017.

ARTICLE 29 DATA PROTECTION WORKING PARTY. «Opinion 02/2013 on apps on smart devices». Brussel·les: Consell d'Europa, 27 de febrer del 2013.

BARLOW , J. P. «A plain text on crypto policy». *Communications of the ACM*, 36(11), novembre de 1993, p. 21-26.

BOE. *Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic*. Madrid: BOE, 12 de juliol del 2002.

BOE. *Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.* Madrid: BOE núm. 298, 14 de desembre de 1999.

BOE. *Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la LOPD*. Madrid: BOE, 19 de gener del 2008.

BOWYER, K. W. *Ethics and Computing: Living Responsibly in a Computerized World*. Los Alamitos, CA, EUA: IEEE Computer Society Press, 1995.

COLMENAREJO FERNÁNDEZ, R. *Una ética para Big Data*. Barcelona: UOC, 2017.

COMISSIÓ EUROPEA. *Major protecció, noves oportunitats: Orientacions de la Comissió sobre l'aplicació directa del Reglament general de protecció de dades a partir del 25 de maig del 2018.* Comunicació de la Comissió al Parlament Europeu i al Consell. Brussel·les: Comissió Europea, 24 de gener del 2018.

COMISSIÓ EUROPEA. *Proposta de Reglament del Parlament Europeu i del Consell sobre el respecte de la vida privada i la protecció de les dades personals en el sector de les comunicacions electròniques i pel qual es deroga la Directiva 2002/58/CE. Reglament sobre la privacitat i les comunicacions electròniques*. Brussel·les: Comissió Europea, 10 de gener del 2017.

CONGRÉS DELS DIPUTATS. *Projecte de Llei orgànica de protecció de dades de caràcter personal*. Madrid: Congrés dels Diputats, 24 de novembre del 2017.

CONSELL DE LA UNIÓ EUROPEA. *Corregendum Reglament general de protecció de dades*. Brussel·les: Consell de la Unió Europea, 19 d'abril del 2018.

CUEVA, DE LA, J. «Código fuente, algoritmos y fuentes del Derecho». *El Notario del Siglo XXI*, 77, maig-juny del 2018.

DAVARA FERNÁNDEZ DE MARCOS, L. *Menores en Internet*. Madrid: AEPD, 2017.

DAVARA RODRÍGUEZ, M. Á. *La protección de datos en Europa*. Madrid: Asnef Equifax, 1998.

DIARI OFICIAL DE LA UNIÓ EUROPEA. *Reglament general de protecció de dades (RGPD)*. 27 d'abril del 2016. Recuperat el 4 d'abril del 2018 de: <https://www.boe.es/doue/2016/119/l00001-00088.pdf>

FISCALIA GENERAL DE L'ESTAT. *Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*. Madrid: 11 de gener del 2013.

FOUCAULT, M. *Vigilar y castigar*. Madrid: Biblioteca Nueva, 2012.

FROSINI, V. *Cibernética, Derecho y sociedad*. Madrid: Tecnos, 1982.

GÁMIZ MEJÍAS, M.; OLTRA GUTIÉRREZ, J. V. (dir.). *Suplantación de identidad en Internet*. València: UPV, 2018.

GARCÍA MIRETE, C. M. *Bases de datos electrónicas internacionales*. València: Tirant lo Blanch, 2014.

GARRIGA DOMÍNGUEZ, A. *Fundamentos éticos y jurídicos de las TIC*. Cizur Menor: Thomson Reuters, 2010.

GOIZUETA VÉRTIZ, J.; GONZÁLEZ MURUA, A. R.; PARIENTE, D. I. *El espacio de libertad, seguridad y justicia: Schengen y protección de datos.* Cizur Menor: Thomson Reuters, 2013.

GÓMEZ SÁEZ, F. «Los reportajes de investigación con cámara oculta y sus repercusiones en los derechos fundamentales», tesi doctoral. Madrid: UNED, 2014.

GRUP DE TREBALL DE L'ARTICLE 29 SOBRE PROTECCIÓ DE DADES. *Directrius sobre el consentiment en el sentit del Reglament (UE) 2016/679*. Brussel·les: Consell de la Unió Europea, 28 de novembre del 2017.

GRUP DE TREBALL DE PROTECCIÓ DE LES PERSONES (GRUP DE TREBALL DE L'ARTICLE 29). *Directrius sobre el consentiment en el sentit del Reglament (UE) 2016/679. 17/SE. WP259 i rev.01*. Brussel·les: 10 d'abril del 2018.

HOBBES, T. *Leviatán*. Barcelona: Losada, 2003.

IDC. *Cómo acelerar el cumplimiento de GDPR*. Madrid: IDC, 2018.

LANDAU, S., *et al.* «Crypto policy perspectives». *Communications of the ACM*, 37(8), agost de 1994, p. 115-121.

LÓPEZ CALVO, J. «Un Reglamento exponente, víctima y resultado de su tiempo». *El notario del siglo XXI* (77), maig-juny del 2018.

MEDINACELLI DÍAZ, K. I. *El tratamiento de lso datos sanitarios*. Madrid: AEPD, 2016.

MIGUEL MOLINA, DE, M.; OLTRA GUTIÉRREZ, J. V. *Deontología y Aspectos Legales de la Informática: cuestiones jurídicas, técnicas y éticas básicas*. València: Servei de Publicacions de la Universitat Politècnica de València, 2007.

MIGUEL MOLINA, DE, M.; OLTRA GUTIÉRREZ, J. V.; Sarabdeen, J. «An exploratory study on the privacy of children's images in Spain's most widely used social network sites (Tuenti and Facebook)». *International Review of Law, Computers&Technology*, 3(24), 2010, p. 277-285.

MOORE , M. (dir). *Sicko* [pel·lícula]. 2007.

NEGROPONTE, N. «Cómo vencer en la revolución digital». Madrid: Conferencia ExpoManagement, 2003.

OLTRA GUTIÉRREZ, J. V. «Echelon hoy». *Novática: Revista de la Asociación de Técnicos de Informática*, 153, 2001, p. 52-55.

ORTEGA Y GASSET, J. *Meditación de la técnica*. Madrid: Revista de Occidente, 1968.

PARLAMENT EUROPEU I CONSELL DE LA UNIÓ EUROPEA. *Directiva (UE) 2016/680 del Parlament Europeu i del Consell, de 27 d'abril del 2016, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les autoritats competents per a finalitats de prevenció*. Brussel·les: Diari Oficial de la Unió Europea, 27 d'abril del 2016.

PARLAMENT EUROPEU I CONSELL DE LA UNIÓ EUROPEA. *Directiva 2003/98/CE del Parlament Europeu i del Consell, de 17 de novembre de 2003, relativa a la reutilització de la informació del sector públic.* Brussel·les: Diari Oficial de la Unió Europea, 31 de desembre del 2003.

PARLAMENT EUROPEU I CONSELL DE LA UNIÓ EUROPEA. *Reglament (CE) núm. 765/2008 del Parlament Europeu i del Consell, de 9 de juliol de 2008, pel qual s'estableixen els requisits d'acreditació i vigilància del mercat relatius a la comercialització dels productes i pel qual es deroga el reglament...* Brussel·les: Diari Oficial de la Unió Europea, 2008.

RINCÓN, R. «El Constitucional extiende el derecho al olvido a las hemerotecas digitales». *El País*, 26 de juny del 2018. Recuperat el 18 de juliol del 2018 de: <https://elpais.com/politica/2018/06/26/actualidad/1530007122_707929.html>.

SALVADOR, P.; RUBÍ, A.; RAMÍREZ, P. «Imágenes veladas». *InDret*, 2011.

SECRETARIA D'ESTAT DE CULTURA. Biblioteca Virtual de Premsa Històrica. Recuperat el 18 de juliol del 2018 de: <http://prensahistorica.mcu.es/es/consulta/busqueda.cmd>

THE INTERNATIONAL TRADE ADMINISTRATION. *European Union: transferring personal data from the EU to the US*. 27 de juliol del 2016. Recuperat el 20 de juliol del 2018 de <https://www.export.gov/article?id=european-union-transferring-personal-data-from-the-eu-to-the-us>

TRIBUNAL DE JUSTÍCIA DE LA UNIÓ EUROPEA. *Google vs Mario Costejá, C-131/12*. Gran Sala del Tribunal de Justícia, 31 de maig del 2014.

TRIBUNAL SUPREM. *Recurso de casación por infracción de preceptos constitucionales e infracción de Ley, STS 1942/2016 - ECLI:ES:TS:2016:1942*. Sala penal del Tribunal Suprem, 3 de maig del 2016.

TRIBUNAL SUPREM. *STS 4132/2015-ECLI:ES:TS:2015:4132 Dret a l'oblit digital. Digitalització d'hemeroteca sense utilitzar codis ni instruccions que...* Tribunal Suprem, sala civil, 15 d'octubre del 2015.

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT. *Bland vs Roberts, Appeal: 12-1671*. doc. 59. 18 de setembre del 2013.

VÁZQUEZ, J. M.; BARROSO, P. *Deontología de la informática. Esquemas*. Madrid: Instituto de Sociología Aplicada, 1992.

WARREN, S. D.; BRANDEIS, L. S. «The Right to Privacy». (T. H. Association, Ed.) *Harvard Law Review*, 4(5), 15 de desembre de 1890, p. 193-220.

Contingut