Protecció de dades

"[…] en el moment que tenen la nostra 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)

El principal objectiu d'aquest tema és oferir un acostament al marc legal de la protecció de dades personals a Europa, amb un especial interès 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 a 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 aquesta per a poder donar-ne compte en el temps reservat pels plans docents, per la qual cosa per a concretar el coneixement amb vista a l'execució pràctica, es fa imprescindible anar al text legal. Perquè els apunts actuals servisquen de full de ruta, quan se cita un dret concret, s'indica quin és l'article de la norma concreta on aquest es pot consultar de manera entera i no resumida.

L'eix que vertebra aquests apunts és el Reglament Europeu de Protecció de Dades, així com el seu reflex en la legislació espanyola, la nostra Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, des d'ara Llei 3/2018, tot i que òbviament no són les úniques normes al·ludides.

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 el 1978 es recollia en la nostra Constitució.

> Article 18 CE
>
> 1. Es garanteix el dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge.
>
> 2. El domicili és inviolable. Cap entrada o registre s'hi pot fer sense consentiment del titular o resolució judicial, excepte en cas de flagrant delicte.
>
> 3. Es garanteix el secret de les comunicacions i, en especial, de les postals, telegràfiques i telefòniques, tret de 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, escoltem que s'identifica amb molts altres termes: privacitat,

intimitat, secret, dret fonamental, llei…, veiem com les paraules "protecció de dades" ens fa pensar en moltes coses.

Potser la resposta rau en el fet que es tracta d'un poc de tot. Parlem d'un dret fonamental, d'una disciplina jurídica, de llei orgànica…, de tot alhora. Encara que per a nosaltres serà, de forma 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 ja quin és el text legal per excel·lència d'aquest tema: el Reglament Europeu de Protecció de Dades (*Diario Oficial de la Unión Europea*, 2016)[1], i fixem-nos en particular en els articles 2n i 3r, on es delimita l'àmbit del Reglament (idèntic al que ens diu l'article 1r de la Llei 3/2018 (BOE, 2018), en endavant ometrem aquestes similituds en nom d'una lectura més lleugera. Si no s'indica altrament, en tot moment els articles i considerants esmentats són referències 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, tot i que amb un llarg seguit d'excepcions. Així, 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 tracta del tractament efectuat per una persona física en l'exercici d'activitats exclusivament personals o domèstiques o quan es tracta d'un tractament realitzat per les autoritats competents amb fins de prevenció, investigació, detecció o enjudiciament d'infraccions penals, o d'execució de sancions penals, inclosa la de protecció enfront d'amenaces a la seguretat pública i la seua prevenció.

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 seues 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 estan a la Unió per un responsable o encarregat no establit a la Unió, quan les activitats de tractament estan relacionades amb l'oferta de béns o serveis, el control del seu comportament, si aquest té lloc a la Unió.

Veiem que apareixen ja paraules que necessiten ser definides: per exemple, el responsable o encarregat del tractament. En unes poques 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 a avançàvem, però que a més queda referendat pel Reglament en el

[1] Com aquesta norma serà emprada de manera exhaustiva, ometrem fins i tot citar-la. 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, tret de cites 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.

primer considerant. I, encara més, s'indica expressament que el tractament de dades personals ha d'estar concebut per a servir la humanitat. Però s'afegeix un matís que ens donarà molt de joc: el dret a la protecció de les dades personals no és un dret absolut sinó que s'ha de considerar en relació amb la seua funció en la societat i mantenir l'equilibri amb altres drets fonamentals, d'acord amb el principi de proporcionalitat. (Considerant 4). Això ja l'avançava (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 ara les activitats relatives a la seguretat nacional. No s'aplica tampoc 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). D'igual manera, no s'aplica tampoc al tractament de dades de caràcter personal per una persona física en el curs d'una activitat exclusivament personal o domèstica (com ara la correspondència, una agenda personal o l'activitat en les xarxes socials). Sí s'aplica als responsables o encarregats del tractament que proporcionen els mitjans per a tractar dades personals relacionades amb aquestes activitats personals o domèstiques (Considerant 18).

Hem de tenir clar que el dret no és un conjunt de disciplines autoexcloents. Moltes vegades se superposen entre si, com en aquest cas, per exemple, succeeix 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. A aquest respecte, 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. Tanmateix, que dos drets no entren en col·lisió és pràcticament utòpic (De Miguel Molina & Oltra Gutiérrez, 2007). En la protecció de dades, normalment s'entrarà 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 resulta evident. Què fem llavors? Els tribunals apliquen en aquest cas el principi de proporcionalitat, ja que caldrà veure en cada cas concret quin dret preval. El dret a la informació no és un dret absolut, com tampoc la llibertat d'expressió, i normalment els jutges i magistrats sempre s'inclinaran 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 enfront del dret a la informació.

Tractament vs llibertat d'expressió

Quin ha de prevaler? No hi ha una recepta única. El Reglament ens diu que s'han de conciliar ambdós, que generaran exempcions o excepcions. (Article 85) Curiosament, un altre article 85,

aquest el de la Llei 3/2018, ens diu expressament que "Tots tenen dret a la llibertat d'expressió a Internet".

La ràpida evolució tecnològica i la globalització han plantejat nous reptes per a la protecció de les dades personals des de l'anterior normativa. S'ha incrementat la magnitud de la recollida i de l'intercanvi de dades personals que permeten que les TIC que empreses privades i autoritats públiques utilitzen dades personals en una escala sense precedents a l'hora de realitzar-ne les activitats. Dades que moltes vegades ixen directament dels usuaris en una difusió voluntària (xarxes socials, per exemple). No cal 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 amb el suport de grans bases de dades mèdiques comença a aplicar-se en plenitud a la medicina, en paral·lel ens assabentem com a la Xina s'és capaç d'identificar 200 persones per minut, estudiar-ne el comportament passat, present i predectiblement futur i atorgar així carnets de bons ciutadans. En aquest món on la intimitat sembla haver-se capgirat com en un calcetí i que es nodreix de *likes* i repiulades és important generar confiança que permeta a l'economia digital desenvolupar-se en tot el mercat interior europeu. Les persones físiques han de tenir el control de les seues dades personals. Cal reforçar la seguretat jurídica i pràctica per a les persones físiques, els operadors econòmics i les autoritats públiques (Considerants 6 i 7). En busca d'aquesta seguretat, i dels drets dels ciutadans, s'ha de minimitzar les diferències en les normes dels països de la Unió, ja que poden constituir un obstacle a l'exercici de les activitats econòmiques en l'àmbit 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 *postures agnòstiques*, que servisquen al fi amb independència del mitjà.

No cal oblidar tampoc un fet que ja heretem d'abans, de normes anteriors (com per exemple 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 seu tractament manual, quan les dades personals costen en un fitxer o estan destinades a ser-hi incloses.

És a dir: una carpeta de gomes amb fitxes de clients…, és un fitxer a protegir.

A pesar d'això, però, hi ha una breu indicació que pot evitar-nos molt de treball tècnic, que per la seua importància no hem d'oblidar: els fitxers o conjunts de fitxers, així com les seues portades, que no estiguen estructurats d'acord amb 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 molt, l'única legislació a tenir en compte a l'hora de tractar amb dades. Respecte a això, resulta interessant la consulta del text de García Mirete (García Mirete, 2014). Per exemple, quan parlem d'ús de dades en comunicacions electròniques, hem de referenciar la LSSI. (BOE, 2002). No hem d'oblidar

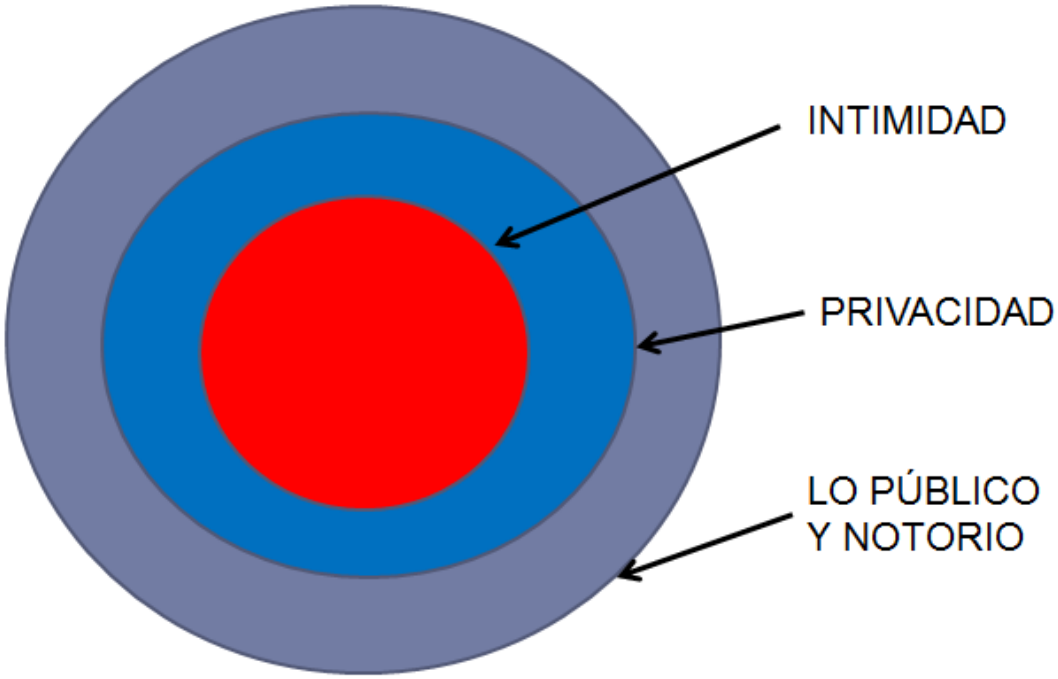
tampoc que les lleis són interpretades pels jutges i moltes vegades hem de parar esment especial a aquestes interpretacions[3].

Per a tancar aquest apartat d'introducció, intentarem eliminar algunes confusions típiques.

La primera d'aquestes és la que ve quan es confonen paraules com ara dades, informació i informàtica. Un dada és difícil que per si sola 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 poc més. La informació és aquesta paret que construïm amb dades, i això ja és un suport ferm. Si sotmetrem la informació a tractament (tractament que sol ser informàtic, per la complexitat que resulta fer manualment accions amb grans quantitats de dades), ja tenim un resultat útil per a un fi determinat. I potencialment perillós, segons siga aquest fi. Amb la informàtica s'ofereixen múltiples possibilitats d'emmagatzematge i tractament de la informació, i de recuperació d'aquesta, de formes tan variades i invisibles per al ciutadà que pot arribar a produir verdadera pressió i control social. El creuament de dades entre bases de dades, amb l'implícit tractament automàtic, provoca en ocasions la pèrdua de control del titular de les dades, que no és ni més ni menys que la persona a qui aquestes dades descriuen.

Però encara queda un altre punt de confusió: totes les dades personals són iguals? Tenen la mateixa importància? Què patim una malaltia degenerativa i es faça públic entre 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 procedeix d'una llista pública? Tot i que aprofundirem en aquest assumpte més endavant, val la pena emprar un gràfic en aquest moment per a establir, a mode de capes, la major o menor incidència en la nostra vida dels distints tipus de dades.

[3] D'exemples, n'hi ha molts. Esmentem-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 núm. 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 on aquest treballava. Es tracta de:
Vulneració de dret a la intimitat, negativa a la cancel·lació de dades, trencament de la garantia de la confidencialitat d'aquestes i inexistència de responsable de fitxer. S'atorga l'empara.
Un últim exemple. Observeu que intencionalment he escollit sentències antigues, anteriors a la mateixa LOPD, perquè es puguen comparar els efectes amb les normes que avui ens regeixen. Sentència 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 als efectes d'embargaments i altres diligències executòries, de manera que han de subministrar dades als serveis estadístics estatals només als efectes d'elaborar estadístiques.



Il·lustració 1. De l'íntim al públic. Elaboració pròpia.

Hem vist de manera molt general què és això de la protecció de dades, què protegeix. I sembla que és una cosa nova, que sorgeix amb les TIC. Però en realitat és un fet de sempre, d'alguna manera ha estat ací. Anem a veure-ho ara.

Un poc d'història

En l'antiga Grècia res semblant a la protecció de dades existia. És a Roma quan apareix el dret de propietat del jo. Es parla d'un home exterior, i l'altre d'interior.

El temps passa, i en l'edat mitjana apareix sant Agustí que parla de l'home com a portador de valors i sant Tomàs d'Aquino que considera la intimitat com un bé sagrat. La privacitat existeix, però es resumeix i recau sobre el *pater familias*. Segueix avançant la història i en l'edat moderna, amb *La raó* i els seus filòsofs, es rebla un poc més el clau. Locke, i el seu concepte de la *llibertat negativa* reconeixen a l'individu una esfera íntima. Rousseau afegeix la intimitat des de l'àmbit de la persona. I amb aquests *rebliments* arribem al segle XX, on comença a jugar la basa un nou participant, la informàtica, i al XXI, on sembla haver-se quedat amb tota la partida.

Avui dia sabem que les dades són propietat del titular, del ciutadà. La informació sadolla les ànsies de poder de molts, ja que poder és informació. La intimitat ara puja de nivell, no solament és ocultament, reserva, sinó la capacitat de decidir en l'esfera íntima.

Veiem com la privacitat, la intimitat de les persones, és un fet que ha preocupat sempre els éssers humans. Fins i tot a les cases romanes on vivia la no-elit, on s'amuntegaven les famílies, les persones buscaven els seus llocs per a la intimitat, secrets particulars que no desitjaven que es feren públics. Però aleshores preocupava més el rumor. Avui és la xarxa de xarxes. Hi ha un

lleu matís. La informàtica ha suposat un instrument important per a tot, bé i malament. Per a trencar aquesta intimitat també. És lògic que cresqueren les normes respecte a això.

A Espanya, per fer una vista ràpida a la nostra particular història del dret, podríem viatjar al passat fins a la Llei d'11 de gener de 1541 on l'emperador Carles I dota d'inviolabilitat les cartes. Un fet que s'estén ja en un moment tan tardà com la Constitució de 1869 a la inviolabilitat de domicili i, per primera vegada, al 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 de 17 juliol de 1945. En el títol preliminar apareix un principi fonamental: el respecte a la dignitat i llibertat humanes. I arribem al marc actual, amb l'any 1978 on la Constitució es promulga, i després de la Constitució, apareixen unes quantes lleis, que van marcant el camí:

- LO 1/1982, de 5 de maig, de Protecció Civil del Dret a l'Honor, a la Intimitat Personal i Familiar i a la Pròpia Imatge
- 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, Llei Orgànica de Regulació del Tractament Automatitzat de les dades de caràcter personal en el 92, llei precedent i quasi mare de la LOPD, Llei Orgànica de Protecció de Dades de caràcter personal, del 99, i a la nostra actual Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals. Però pel camí van sorgint algunes lleis que matisen uns quants aspectes. Per exemple:

- Llei 34/2002, d'11 de juliol, de Serveis de la Societat de la Informació i de Comerç Electrònic (LSSI).
- Llei 56/2007, de 28 de desembre, de Mesures d'Impuls de la Societat de la Informació.
- Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions. (Llei *ad hoc* per a la lluita contra el terrorisme i crim organitzat.)
- Llei 9/2014, de 9 de maig, General de Telecomunicacions.

Podríem fer molt, molt més llarga aquesta llista. Però per a definir concretament el nostre marc, deixem clar l'essencial, partint d'aquesta pedra basal que és l'article 18 de la Constitució:

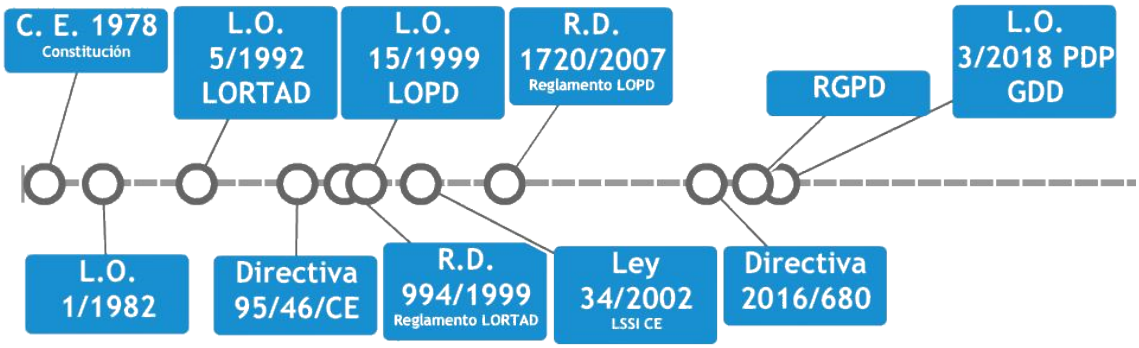
> *4. La llei limitarà l'ús de la informàtica per a garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets.*

Amb aquest parc punt de partida, aparegué al seu moment, condicionat pel protocol de Schengen, *Espacio de Libertad, Seguridad y Justicia*) (Goizueta Vértiz, González Murua, & Pariente, 2013) la nostra extinta LORTAD, Llei Orgànica 5/1992, de 29 d'octubre. Llei que va ser

modificada mitjançant el Reial Decret 1332/1994, de 20 de juny, pel qual es despleguen determinats aspectes de la LORTAD i reglamentada amb el Reial Decret 994/1999, d'11 de juny, Reglament de Mesures de seguretat dels fitxers automatitzats que continguen dades de caràcter personal. És a dir: a poc a poc el legislador va construint l'edifici legal.

I quan semblava acabat, una Directiva Comunitària (95/46/CE de 24 d'octubre de 1995) exigia l'extensió a fitxers manuals. Això provocà 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 desplegament de la Llei Orgànica 15/1999. Llei que ja ha quedat obsoleta, per la necessària entrada en vigor del Reglament Europeu de Protecció de Dades, que ens ha portat fins a l'actual Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

Podem veure un fil temporal en la imatge següent:



Il·lustració 2. Legislació principal sobre protecció de dades que afecta Espanya (elaboració pròpia)

I què ocorria al *món*, fora de les nostres fronteres?

En els ordenaments d'àmbit anglosaxó se li anomenat *privacy*, ací espanyolitzat com "privacidad" (Davara Rodríguez, 1998). No és exactament igual, però atenent la segona accepció del diccionari de la RAE ("Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión), podem establir per al nostre treball una certa identitat. (Real Academia Española, 2017). Cal indicar que, si rastregem textos de l'altra banda de l'Atlàntic escrits en anglès amb el terme *privacy* podem observar algunes diferències, que no és moment de relacionar.

Quan se xifra l'origen de la privacitat en el món anglosaxó?

Sembla haver-hi una coincidència generalitzada a indicar que foren Samuel D. Warren i Louis D. Brandeis (Warren & Brandeis, 1890) els que en el seu *Dret a la privacitat* fonamentaren en el principi d'inviolabilitat a la persona els límits jurídics a la intromissió en la vida d'aquestes. Garriga (Garriga Domínguez, 2010) indica que poc després de l'aplicació es comença a usar per un tribunal de Nova York que empra l'expressió encunyada (*the right to privacy*), que a partir d'aquell moment es multiplicaria en resolucions judicials (tot i que també s'usarà amb el curiós nombre de "Dret a ser deixat en pau").

Als Estats Units (seguim Garriga en aquest punt) William Prosser publica el 1960 un assaig usant les línies mestres de Warren i Brandeis, que assenten les possibles violacions del dret a la intimitat en la societat moderna. L'any següent, 1961, la idea salta 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 a Espanya Pérez Luño, que divulguen al llarg dels dos continents aquestes idees. (Garriga Domínguez, 2010). Cal precisar, ja que hem esmentat diferències entre ambdós conceptes, 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 el 1948 el dret a la intimitat s'arreplega en l'article 12 de la Declaració dels drets humans, i molt poc després, es reflecteix en l'article 8 del Conveni de Roma, el 1950.

Al maig de 1967, 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 seua influència 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 les noves fites científiques i tècniques".

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

El món continua girant i el 1970, el 23 gener, sorgeix la resolució 428 de l'Assemblea Consultiva del Consell d'Europa: "Intimitat com un objecte d'obligada protecció enfront de la intromissió de la tecnologia de la informació". Això dona pas perquè el 1973 sorgisca la resolució (22) de 26 de setembre: "Protecció de la vida privada de les persones físiques enfront del sector privat" i el 1974(29) igualment, sobre el sector públic. Es poden veure unes interessants reflexions sobre les resolucions 1973(22) i 1974(29) en el text de Davara referenciat en la bibliografia (Davara Rodríguez, 1998). És el moment en què comencen a inspirar-se alguns estats, com ara l'alemany, per a aprovar lleis com és la de Hesse, de 1970, que busca protegir el dret de la personalitat restringint la utilització de dades personals que puguen afectar els ciutadans per l'Administració. Aviat, el 1974, es promulga la primera Privacy Act dels Estats Units de Nord-amèrica. En aquesta etapa s'introdueix la idea de la protecció efectiva a les persones enfront de l'ús informatitzat de les dades. Una tercera etapa està marcada per 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 del 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 el 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.

En aquest mateix 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.

En aquest resum a rajaploma hem deixat de mencionar sentències interessants, com la que desplega el "principi de consentiment" o el "dret d'autodeterminació", procedents del Tribunal Constitucional alemany, de 1983, que inspiraren la llei alemanya de 1990 i que des de llavors s'expandí 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: avui és concep com una llibertat positiva, la llibertat d'exercir un dret de control sobre les dades referides a la mateixa persona que ja han eixit de l'esfera de la intimitat per a esdevenir 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 aquells ossos polars que porten incorporat un radiotransmissor en miniatura que permet que les seues passes es registren i envien a un satèl·lit. Els grans bancs de dades de les administracions públiques i grans corporacions que apareixen en aquestes dades feren possible una vigilància real de la vida quotidiana, que 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 dona pas al que Frosini (Frosini, 1982) ha denominat la llibertat informàtica: el dret a autotutela de la pròpia identitat informàtica; és a dir, la que resulta de la recollida, de la confrontació de les dades personals inserides en un sistema informàtic. El respecte a la intimitat s'estén avui a una esfera àmplia de la vida privada. No solament es tracta d'informes íntims sinó també d'alguns comportaments personals, elements distints de la personalitat, opinions religioses i polítiques…, dades anomenades sensibles per a distingir-les de les que estan a disposició del públic. Pensem que allò que en un principi resultava poc cridaner, l'obtenció d'informació creuant dades, creant perfils, ha esdevingut pràcticament un dels eixos de la legislació actual.

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

Es tracta ja de llibertat de controlar l'ús de les pròpies dades personals 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 la difusió…, és, en si, una última etapa, on ens preocupa la incidència d'internet i els avanços científics, com ara el desxiframent del mapa genètic.

Però tornem al principi: ens preguntàvem, és un Dret fonamental, una disciplina jurídica? Tractem de respondre-hi.

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

És una disciplina jurídica? Abundants textos (vegeu la bibliografia) l'interpreten com una disciplina jurídica que busca protegir la intimitat i altres drets fonamentals de les persones físiques enfront del risc que suposa la recopilació i l'ús indiscriminat de les seues dades personals, de manera que abraça tot tipus de tractament (independentment que es realitze de manera manual o informatitzada) i marca la necessitat de desplegar normes que, limitant l'ús de les dades personals, garantisquen l'honor i la intimitat personal i familiar dels ciutadans.

Amb un sí rotund a ambdues preguntes, seguim endavant.

Marc legal bàsic

L'eix en què ens mourem en el tema actual és doble: el Reglament Europeu de Protecció de Dades (RPGD des d'ara) i la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (3/2018 des d'ara). Un eix doble, però que veurem que en realitat és convergent, ja que la Llei 3/2018 està plena d'al·lusions al RGPD, que en algun cas matisa i en d'altres complementa.

Al llarg de la resta del tema farem al·lusió quasi en exclusiva a aquestes dues normes. Però cal indicar que no són les úniques d'interès, així que almenys tractarem d'enumerar les de més interès (incloent-hi també normativa tècnica) i donar consells per a una consulta eficaç i actualització.

El millor dels consells és anar a la zona de codis del *Butlletí Oficial de l'Estat* (BOE, 2019). En aquesta part de descàrrega podem trobar, entre d'altres, els codis relatius a la Protecció de Dades de Caràcter Personal i al Dret a l'Oblit, que prompte veurem com ens és de molt d'interès.

Per a cadascun dels codis podem tenir una descàrrega, en formats pdf o epub, i sempre actualitzada, de tota la legislació rellevant: des de les lleis principals fins a les resolucions i instruccions de l'Agencia Española de Protección de Datos, als fragments d'altres lleis que s'han de tenir en compte per qualsevol implicat en aquests assumptes. A més, podem accedir de manera alternativa al text consolidat i a les versions anteriors de les normes, fet que en algun moment pot ser de molt d'interès, sobretot en tasques d'auditoria i consultoria.

Il·lustració 3. Zona de descàrrega de codis en el web del "Boletín Oficial del Estado". Elaboració pròpia.

Es tracta de documents molt grans, de vora les cinc-centes i mil pàgines cadascun, però precisament per la seua completesa (i actualització) són de màxim interès.

Entre les normes nacionals d'interès, destaquen (tot localitzable a través del web del BOE):

- Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic.
- 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 pròpia imatge.
- Reial Decret Llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació. Aquest RD és d'alta importància, no solament perquè en tot moment s'estableix la relació necessària entre l'Agencia Española de Protección de Datos i els responsables de la seguretat, sinó per la seua disposició addicional tercera (Notificació de violacions de seguretat de les dades personals a través de la plataforma comuna prevista en aquest reial decret llei) que indica que la plataforma comuna per a la notificació d'incidents prevista en aquest reial decret llei es podrà emprar per a la notificació de vulneracions de la seguretat de dades personals segons el Reglament (UE) 2016/679 (RGPD), en els termes que acorden l'Agencia Española de Protección de Datos i els òrgans que gestionen la dita plataforma.
- Circular 1/2019, de 7 de març, de l'Agencia Española de Protección de Datos, sobre el tractament de dades personals relatives a opinions polítiques i enviament de propaganda electoral per mitjans electrònics o sistemes de missatgeria per partits polítics, federacions, coalicions i agrupacions d'electors a l'empara de l'article 58 bis de la Llei Orgànica 5/1985, de 19 de juny, del Règim Electoral General.

No cal descartar la normativa autonòmica i, en concret, el que emanen les agències autonòmiques de protecció de dades. A aquest respecte és d'interès la llei basca de Protecció de Dades (LLEI 2/2004, de 25 de febrer, de Fitxers de Dades de Caràcter Personal de Titularitat Pública i de Creació de l'Agencia Vasca de Protección de Datos). Amb vista a enfocar el títol X

de la Llei 3/2018, cosa que farem més endavant en aquest tema, pot ser d'interès consultar la Llei 10/2017, de 27 de juny, de les voluntats digitals i de modificació dels llibres segon i quart del Codi civil de Catalunya.

Respecte de la legislació europea, considerem que no solament el RGPD és l'únic reglament a considerar emanat de la Unió. Entre altres reglaments (i directives i recomanacions) d'interès figuren (tot això localitzable des del cercador legal del dret de la UE, EUR-lex (EUR-Lex, 2019)):

- Reglament (UE) núm. 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014 , relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior (comunament anomenat el reglament EIDAS).
- Reglament (UE) núm. 611/2013 de la Comissió, de 24 de juny de 2013, relatiu a les mesures aplicables a la notificació de casos de violació de dades personals en el marc de la Directiva 2002/58/CE del Parlament Europeu i del Consell sobre la privacitat i les comunicacions electròniques.
- Directiva (UE) 2016/680 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per les autoritats competents per a fins de prevenció, investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals, i a la lliure circulació de les dites dades.
- Directiva (UE) 2015/2366 del Parlament Europeu i del Consell, de 25 de novembre de 2015, sobre serveis de pagament en el mercat interior.
- Dictamen 02/2013 sobre les aplicacions dels dispositius intel·ligents, de molt d'interès per a qui treballa amb aplis per a mòbils, per exemple.
- Directrius sobre el consentiment en el sentit del Reglament (UE) 2016/679 adoptades el 10 d'abril de 2018.
- Directrius sobre l'avaluació d'impacte relativa a la protecció de dades (EIPD) i per a determinar si el tractament «implica probablement un alt risc» a efectes del Reglament (UE) 2016/679. Adoptades el 4 d'octubre de 2017.
- Directrius sobre la notificació de les violacions de la seguretat de les dades personals d'acord amb el Reglament 2016/679. Adoptades el 6 de febrer de 2018.
- Comunicació de la Comissió al Parlament Europeu i al Consell "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 de 2018".
- Resum del Dictamen sobre la proposta de Directiva relativa a determinats aspectes dels contractes de subministrament de continguts digitals (2017/C 200/07).
- 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 (e-privacy).

Entrem ara en un altre camp de molt d'interès per al professional, quasi podríem arriscar-nos a dir que superior al simple coneixement legal: les normes (UNE, ISO, etc.) de caràcter tècnic que són o poden ser d'interès en distints moments del treball del professional informàtic. Intentarem categoritzar-les per treballs, i destacarem així les normes més importants per a:

- Realitzar anàlisis de riscos

    - ISO/IEC 29187-1:2013. Information technology - Identification of privacy protection requirements pertaining to learning, education and training (LET) - Part 1: Framework and reference model
    - ISO/IEC TR 29110-5-2-1:2016. Systems and software engineering - Lifecycle profiles for Very Small Entities (VSEs) - Part 5-2-1: Organizational management guidelines
    - ISO/IEC TR 29110-5-6-1:2015. Systems and software engineering - Lifecycle profiles for Very Small Entities (VSEs) - Part 5-6-1: Systems engineering - Management and engineering guide: Generic profile group: Entry profile
    - ISO/IEC TR 29110-5-6-2:2014. Systems and software engineering - Lifecycle profiles for Very Small Entities (VSEs) - Part 5-6-2: Systems engineering - Management and engineering guide: Generic profile group: Basic profile
    - ISO/IEC 29100:2011. Information technology - Security techniques - Privacy framework
- Actuacions en descobrir una bretxa de seguretat
    - UNE 71505-1:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales.
    - UNE 71505-2:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas.
    - UNE 71505-3:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 3: Formatos y mecanismos técnicos.
    - ISO/IEC 29100:2011. Information technology - Security techniques - Privacy framework (sí, una altra vegada).
    - ISO/IEC 29147:2018. Information technology - Security techniques - Vulnerability disclosure.
- Destrucció de material sensible
    - UNE-EN 15713:2010. Destrucción segura del material confidencial. Codi de buenas prácticas.
- De forma general
    - UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incloent-hi Cor 1:2014 i Cor 2:2015)
        - ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements
        - ISO/IEC 27001:2013/Cor 1:2014
        - ISO/IEC 27001:2013/Cor 2:2015
    - ISO/IEC 27013:2015. Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
    - ISO/IEC 27009:2016. Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements

    - ISO/IEC TR 27023:2015. Information technology — Security techniques — Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

Guies d'interès de l'Agencia Española de Protección de Datos i altres entitats. (Totes aquestes guies estan disponibles en el web de l'agència o de la institució que s'indique, i si en algun moment una d'aquestes desapareix es deu a l'actualització necessària del material. Es recomana la cerca en el web de l'agencia, el títol indicat és el que s'empra literalment en les guies, per a facilitar-ne la localització):

- Per al professional, atenent a la seua figura:
    - Directrius per a l'elaboració de contractes entre responsables i encarregats del tractament.
    - Guia del responsable de fitxers.
    - Guia del Reglament General de Protecció de Dades per a responsables de tractament.
- Per al professional, atenent a labors concretes:
    - Guia sobre l'ús de galetes
    - Guia pràctica d'anàlisis de riscos en els tractaments de dades personals subjectes al RGPD.
    - Orientacions sobre protecció de dades en la reutilització de la informació del sector públic.
    - Guia de seguretat de dades.
    - Guia per a la gestió i notificació de bretxes de seguretat.
    - Guia per al compliment del deure d'informar.
    - Guia pràctica per a les avaluacions d'impacte en la protecció de les dades subjectes al RGPD.
        - Hi ha en l'Agència Catalana de Protecció de Dades una guia de molt d'interès sobre això amb nom similar: Guia pràctica d'Avaluació d'impacte relativa a la protecció de dades.
        - També en una altra agència, la francesa, el CNIL, hi ha un material molt interessant: no solament guies, sinó un programari que es pot executar al vol, que dona suport al professional en aquest treball, disponible en espanyol (Comisión Nacional de Informática y de las Libertades, 2019).
    - Llista de compliment normatiu (una de les millors eines, un gran llista de comprovació (*checklist*) que cap professional es pot permetre el luxe d'ignorar)
- Per a elements molt específics, però delicats:
    - Fingerprint o empremta digital del dispositiu.
    - Guia per a clients que contracten serveis d'informàtica en núvol (*Cloud Computing*).
    - Protecció de dades i administració local.
    - Protecció de dades i prevenció de delictes.
    - De l'Agència Catalana de Protecció de Dades cal destacar-ne les Pautes de protecció de dades per als centres educatius (Agencia Catalana de Protección de Datos, 2018).

    - Sobre la cadena de blocs o *blockchain*, el CNIL té un document de molt d'interès: Solutions for a responsible use of the blockchain in the context of personal data.
- També hi ha guies orientades als ciutadans. Destaquem la Guia per al ciutadà. En aquest sentit cal destacar l'esforç de divulgació que fa l'Agencia mantenint el programa setmanal en Radio Nacional de España "Protegemos tu privacidad" (RNE, 2019).

De la molta bibliografia existent, es pot destacar un petit gran llibre de Delgado y Puyol: *La Implantación del Nuevo Reglamento General de Protección de Datos de la Unión Europea* (Delgado Carravilla & Puyol Montero, 2018).

Deixem de banda comentar sentències d'interès, per excedir del propòsit d'aquest tema.

Figures professionals i actors a considerar

Són molt els actors possibles en la gestió i protecció de les dades personals. En aquest apartat ens centrarem en els tres més rellevants, amb un ampli desplegament legal, encerclant-los. Parlem de l'encarregat del tractament, del responsable del tractament i del delegat de protecció de dades.

Comencem amb unes breus definicions per a cadascuna d'aquestes figures:

Responsable del tractament o «responsable»: la persona física o jurídica, autoritat pública, servei o un altre organisme que, sol o junt amb altres, determine els fins i mitjans del tractament; si el Dret de la Unió o dels estats membres determina els fins i mitjans del tractament, el responsable del tractament o els criteris específics per al seu nomenament podrà establir-los el Dret de la Unió o dels estats membres;

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

Delegat de protecció de dades (DPD o DPO, segons s'empren les sigles en valencià o en anglès): Especialista en matèria de protecció de dades, que ocuparà un lloc junt amb les figures del responsable i encarregat del tractament. Aquesta figura apareix en la legislació arran del Reglament Europeu de Protecció de Dades, mentre que les altres dues tenen ja la seua breu història darrere. És l'encarregat del tractament de les obligacions legals en la matèria de protecció de dades de l'organització que el contracte, i serà el garant del compliment del RGPD. Assessorarà, doncs, l'organització, s'assegurarà que es complisca amb les obligacions en protecció de dades i actuarà d'interlocutor amb l'Agencia Española de Protección de Datos i amb qualsevol ciutadà que vulga exercir-ne els drets davant de l'organització.

Responsable del tractament (Article 24)

Després de la definició, perfilem-ne el rol.

Considerant naturalesa, àmbit, context, fins del tractament i riscos, el responsable del tractament aplicarà, revisarà i actualitzarà mesures tècniques i organitzatives apropiades a fi de garantir i poder demostrar que el tractament està d'acord amb el Reglament. L'adhesió a

codis de conducta o a un mecanisme de certificació podran ser utilitzats com a elements per a demostrar el compliment de les obligacions pel responsable del tractament.

Atès que ens movem en un àmbit d'actuació europeu, s'ha de determinar si és evident que el responsable (o l'encarregat) actua en aquest àmbit. 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 resideix el responsable del tractament, són indicadors, però no n'hi ha prou per a determinar la dita intenció. Es poden considerar factors, com ara l'ús d'una llengua o una moneda utilitzada generalment en un o diversos estats membres, o la menció de clients o usuaris que resideixen a la Unió (Considerant 23).

Una figura relacionada és la de **corresponsable del tractament** (Article 26). Aquesta es dona quan dos o més responsables determinen conjuntament els objectius i els mitjans del tractament. Si és el cas, s'ha de determinar de manera transparent i de mutu acord les seues responsabilitats respectives, i els aspectes essencials d'aquest acord es posaran a disposició dels interessats.

Una altra figura digna de menció és la dels **representants de responsables o encarregats no establits a la Unió** (Article 27). S'ha de designar per escrit un representant a la Unió, però això es pot obviar si el tractament és ocasional, no inclou maneig a gran escala de categories especials de dades i és improbable que implique un risc per als drets i llibertats de les persones físiques o les autoritats o organismes públics. En tot cas, aquesta designació s'entendrà sense perjudici de les accions que es puguen emprendre contra el mateix responsable o encarregat.

Encarregat del tractament (Articles 28 i 29)

Igual que amb el responsable del tractament n'hem de perfilar el rol.

El responsable del tractament elegirà un encarregat que oferisca garanties suficients per a aplicar mesures tècniques i organitzatives apropiades. L'encarregat del tractament al seu torn no recorrerà a un altre encarregat sense l'autorització prèvia per escrit, específica o general, del responsable.

El tractament per l'encarregat es regirà 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 estipula:

- que l'encarregat tractarà les dades personals únicament seguint instruccions documentades del responsable (incloent-hi transferències a un tercer país);
- garantirà que les persones autoritzades per a tractar dades personals s'hagen compromès a respectar la confidencialitat;
- assistirà el responsable, tenint en compte la naturalesa del tractament, a través de mesures tècniques i organitzatives apropiades, sempre que siga possible, perquè aquest puga complir amb la seua obligació de respondre a les sol·licituds;
- a elecció del responsable, suprimirà o retornarà totes les dades personals una vegada finalitze la prestació dels serveis de tractament i suprimirà les còpies existents, tret que es requerisca la conservació de les dades personals;
- posarà a disposició del responsable tota la informació necessària per a demostrar

el compliment de les obligacions establides i permetrà i contribuirà a la realització d'auditories.

Sobre aquest contracte, l'autoritat de control podrà adoptar clàusules contractuals tipus. Constarà per escrit (p. e. de forma electrònica). Si un encarregat del tractament infringeix el Reglament en determinar els fins i mitjans del tractament, serà considerat responsable del tractament respecte al dit tractament.

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

Proposta:

Localitza clàusules contractuals tipus en el web de l'Agencia Española de Protección de Datos (Agencia Española de Protección de Datos, 2018)

Cal destacar que tant el responsable com l'encarregat del tractament i els seus representants cooperaran amb l'autoritat de control que ho sol·licite en l'exercici de les seues funcions. (Article 31)

Delegat de protecció de dades (Articles 37 i 38)

Ja hem dit que es tracta de les més recents de les figures (tot i que en la legislació alemanya ja existia). El seu perfil ha de ser un especialista en dret de protecció de dades, amb unes funcions que li fan semblar una mena de síndic de greuges de les dades. Aquestes serien, bàsicament (Article 39):

- Informar i assessorar els responsables i encarregats del tractament de dades personals (i els seus empleats) sobre 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 implique un alt risc per als drets i llibertats de les persones físiques, i supervisar-ne després l'aplicació.
- Cooperar amb les "autoritats de control" (és a dir, amb les agències de protecció de dades).
- Servir de finestreta o punt de contacte de les autoritats de control per a qualsevol consulta sobre el tractament de dades personals.

Així com el tractament de dades implica sempre l'existència d'un encarregat i un responsable, amb els DPD no sempre els trobarem. Només fan falta quan el tractament el porta a cap una autoritat o organisme públic (excepte tribunals), o quan les operacions de tractament pel que fa a la seua naturalesa, abast i/o fins requerisquen una observació habitual i sistemàtica d'interessats a gran escala, o si aquestes consisteixen en el tractament a gran escala de categories especials de dades personals i de dades relatives a condemnes i infraccions penals.

En resum: cal 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? El nivell de coneixements especialitzats necessari s'ha de determinar en funció de les operacions de tractament de dades que es porten a cap i de la protecció exigida per a les dades personals tractades pel responsable o l'encarregat (Considerant 97). Exercirà 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 fins del tractament.

Podrà formar part de la plantilla del responsable o de l'encarregat del tractament o exercir-ne les funciones en el marc d'un contracte de serveis. En tot cas, tindrà una relació fluida amb el responsable i l'encarregat del tractament, els quals garantiran que el delegat de protecció de dades participe de forma adequada i en temps oportú en totes les qüestions relatives a la protecció de dades personals. Li facilitaran els recursos necessaris per a l'exercici de les seues funcions i l'accés a les dades personals i a les operacions de tractament, per al manteniment dels seus coneixements especialitzats i garantirà que no rep cap instrucció pel que fa a l'exercici de les seues funcions. Retrà comptes directament al més alt nivell jeràrquic del responsable o encarregat.

Recordem que exerceix de *finestreta* respecte als interessats 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 el secret, tot i que podrà exercir altres funcions i comeses (que no han de produir conflicte d'interessos).

Articles de màxim interès per a entendre la figura del delegat de protecció de dades:

Article 34 de la Llei 3/2018. Designació d'un delegat de protecció de dades.

Article 35 de la Llei 3/2018. Qualificació del delegat de protecció de dades.

Article 36 de la Llei 3/2018. Posició del delegat de protecció de dades.

Article 37 de la Llei 3/2018. Intervenció del delegat de protecció de dades en cas de reclamació davant de les autoritats de protecció de dades.

RGPD Article 37. Designació del delegat de protecció de dades.

RGPD Article 38. Posició del delegat de protecció de dades.

RGPD Article 39. Funcions del delegat de protecció de dades.

Definicions. Principis de la llei

Convé abans d'entrar en definicions que centrem què s'espera del tractament de dades. Entra en joc una paraula (*qualitat*) que pot portar-nos imatges molt diferents. Per a un espectador aliè a la llei, pot ser que la primera impressió de la qualitat de les dades siga que aquestes han de ser com més completes i exhaustives millor. Però aquest espectador 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 el fi perseguit, per

la qual cosa han de ser adequades i no excessives.

- Finalitat: Només es poden recollir i tractar les dades que siguen adequades amb l'àmbit i finalitats determinades, explícites i legítimes per a les que s'han obtingut.
- Veracitat i exactitud: Les dades han de ser exactes i posades al dia 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 han de ser recollides sense enganys o falsedats per qui les sol·licita.
- Seguretat: S'han d'adoptar les mesures necessàries per a garantir la seguretat de les dades personals i evitar alteració, pèrdua, tractament o accés no autoritzats.

Si anem a l'article 5 del Reglament, trobarem els principis establits per la llei, que veurem que són pràcticament un eco d'això que avançàvem. Així, en l'article esmentat trobem les exigències següents:

- Licitud, lleialtat i transparència;
- Limitació de la finalitat: recollides amb fins determinats, explícits i legítims, i no seran tractats ulteriorment de manera incompatible amb els dits fins;
- Minimització de dades: adequades, pertinents i limitades a la informació necessària en relació amb els fins per als quals es tracten;
- Exactitud: exactes i actualitzades;
- Integritat i confidencialitat: es garanteix una seguretat adequada de les dades personals.

Hem d'afegir, 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 els termes que puguen ser més confusos.

La **"licitud del tractament"** (vegeu l'article 6). El tractament només serà lícit si es compleix almenys una de les condicions següents: o bé l'interessat donà el seu consentiment per al tractament de les seues dades personals per a un o diversos fins específics, o bé el tractament és necessari per a l'execució d'un contracte en què 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 realitzada 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 els dits 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 infant.

Quan el tractament per a un altre fi distint d'aquell per al qual es recolliren 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 tindrà en compte, entre d'altres, qualsevol relació entre els fins per als quals s'han recollit les dades personals i els fins del tractament ulterior previst; el context en què s'han recollit 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 podran incloure el xifratge o la pseudonimització[4].

Parlem ara de l'**exactitud de les dades**. Quan parlem de dades exactes (i, si cal, actualitzades) s'ha de lligar el concepte al fi que es tracta. Un dada desactualitzada d'una adreça pot ser inexacta per a enviar una comunicació, però no a fins històrics, per exemple. És deure del responsable mantenir l'exactitud, per a la qual cosa ha d'incorporar totes les mesures raonables perquè se suprimisquen o rectifiquen sense dilació, la inexactitud de les dades personals, excepte si venen així directament de l'afectat o s'han obtingut d'un mediador o intermediari que és qui assumirà les responsabilitats que se'n puguen derivar en el supòsit de comunicació al responsable de dades que no es corresponen amb les facilitades per l'afectat. D'igual manera, no seria tampoc responsabilitat seua si s'han obtingut d'un altre responsable en virtut de l'exercici per l'afectat del dret a la portabilitat o si s'han obtingut d'un registre públic. Aquests principis fonamentals podem seguir-los en els articles 4 i 11 de la Llei 3/2018 i en l'article 12 del RGPD i l'apartat 5.1.d)

Sobre aquests dos punts, lligant-los moltes vegades, figura la **transparència**. El responsable del tractament prendrà les mesures oportunes per a facilitar a l'interessat tota la informació (indicada en els articles 13 i 14) en forma concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill, en particular qualsevol informació dirigida específicament a un infant. La informació serà facilitada per escrit o per altres mitjans, inclusivament, si pertoca, per mitjans electrònics. Quan ho sol·licite l'interessat, la informació es podrà facilitar verbalment sempre que es demostre la identitat de l'interessat per altres mitjans. La informació facilitada, com tota comunicació són a títol gratuït. Quan les sol·licituds siguen manifestament infundades o excessives, especialment pel seu caràcter repetitiu, el responsable del tractament podrà cobrar un cànon raonable o negar-se a actuar respecte de la sol·licitud. Aquest principi fonamental podem seguir-lo de nou en els articles 4 i 11 de la Llei 3/2018 i en l'article 12 del RGPD i els apartats 5.1.d). i 5.1.f)

És un interès legítim dels usuaris la necessitat de saber si un sistema informació és capaç de resistir, en un nivell determinat de confiança, a 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 oferits per aquests o accessibles a través d'aquests sistemes i xarxes, per autoritats públiques, equips de resposta a emergències informàtiques (CERT), equips de resposta a incidents de seguretat

[4] Entendrem per pseudonimització el procediment mitjançant el qual es reemplacen camps d'informació personal dins d'un registre de dades per un o més identificadors artificials (pseudònims) per a aconseguir així que cada registre siga menys identificable, però igualment apte per al processament. El Reglament ho ofereix com a alternativa a l'anonimització (considerem que aquest és un procés irreversible, i les dades personals deixen de ser identificables, amb l'avantatge d'evitar el dret a l'oblit ja que realitza una supressió completa, amb la qual cosa podem continuar generant mètriques clau per al negoci). Una possible pseudonimització és el xifratge, que no es pot revertir sense la clau de desxifratge). En aquest cas, aquesta clau s'ha de guardar per separat 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, apareixen a l'apartat "Definicions" d'aquest mateix tema.

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).

En tot moment, recordem el sumatori:

ADEQUADES + PERTINENTS + NO EXCESSIVES = QUALITAT

Definicions

Una vegada assentats els principis, passem a les definicions. En l'article 4 del Reglament Europeu se'ns dona un seguit de definicions que conformaran les rajoles amb què construïm les idees d'aquest tema. Directament d'allí, tan sol introduint alguna nota aclaridora, portem aquestes. Cal fer una apreciació: les definicions semblen mostrar-se com les cireres d'un cistell, ja que quan en prens una et portes penjades unes quantes més. Podem veure això clarament en la primera d'aquestes, "dades personals", on per a definir el terme alhora es defineix que és una persona física identificable i, per enumeració, un identificador. Així, es parla de:

Dades personals: tota informació sobre una persona física identificada o identificable («l'interessat»); es considerarà persona física identificable qualsevol persona amb una identitat que es puga determinar, directament o indirectament, en particular mitjançant un identificador, com per exemple un nom, un nombre 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 de la dita persona;

Hem de tenir en compte que una dada, en si, no és bona ni dolenta, ni assenyala ni deixa d'assenyalar. Sol ser la unió entre dades el que ens preocupa, tot i que a vegades també ho fan dades soltes. Un exemple: òbviament no és igual dir 65, que "Vicent Bonastre Bru té 65 anys". Un exemple més ampli en la taula següent:

Dades aïllades no afectades	Dades afectades
1979	Albert Martínez Pujol
46071	http:\\www.pepmascarell.net
95%	158.153.205.26
Barcelona	C\ Nou, 23, pta. 18
Groc	kike.moreno@gmail.com

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

Tractament: qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, ja siga per procediments automatitzats o no, com ara la recollida, registre, organització, estructuració, conservació, adaptació o modificació, extracció, consulta, utilització, comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, confrontació 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. Recollida
2. Tractament en si (creuament, relació...)
3. Utilització i, si és el cas, comunicació (cessió)

Limitació del tractament: el marcatge de les dades de caràcter personal conservades a fi de limitar-ne el tractament en el futur;

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

Aquestes llistes s'elaboren amb totes les garanties legals per la Federació Espanyola de Comerç Electrònic i Màrqueting Directe, de manera que realitzen unes llistes de possibles clients en funció de les seues 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 a cada moment.

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

Per a apuntar-s'hi, n'hi ha prou amb accedir a la URL: https://www.listarobinson.es/

Elaboració de perfils: qualsevol 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 de la dita persona física;

Pseudonimització: correspon al tractament de dades personals realitzat de manera tal que ja no es puguen atribuir a un interessat sense utilitzar informació addicional, sempre que la dita informació addicional conste per separat 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 d'acord amb criteris determinats, ja siga centralitzat, descentralitzat o repartit de forma funcional o geogràfica;

Alerta: segons aquesta definició, un fitxer convencional amb les dades dels clients escrits a mà en fitxes ordenades alfabèticament és precisament això, un fitxer. Amb tot el que suposa.

Destinatari: la persona física o jurídica, autoritat pública, servei o un altre organisme a què es comuniquen dades personals, es tracte o no d'un tercer. Tanmateix, 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 les dites autoritats públiques serà conforme a les normes en matèria de protecció de dades aplicables als fins del tractament;

Tercer: persona física o jurídica, autoritat pública, servei o organisme distint 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: qualsevol manifestació de voluntat lliure, específica, informada i inequívoca per la qual l'interessat accepta, ja siga mitjançant una declaració o una clara acció afirmativa, el tractament de dades personals que li concerneixen;

Violació de la seguretat de les dades personals: qualsevol 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 forma o la comunicació o 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 d'aquesta persona, obtingudes en particular de l'anàlisi d'una mostra biològica d'aquesta persona;

Què serien les dades genètiques? Es tractaria 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 de la dita 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 el seu estat de salut;

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 recollida en ocasió de la seua inscripció a efectes d'assistència sanitària, o en ocasió de la prestació d'aquesta assistència; tot número, símbol o dada assignats 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 seua font, per exemple un metge o un altre professional sanitari, un hospital, un dispositiu mèdic o una prova diagnòstica *in vitro* (Considerant 35).

Com es pot entendre, hi ha dades genètiques i dades biomètriques que encaixarien en aquesta mateixa categoria.

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 (DOL 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, tret que les decisions sobre els fins 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 considerarà establiment principal. Quant 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 tinguera aquesta, l'establiment de l'encarregat a la Unió en què es realitzen les principals activitats de tractament en el context de les activitats d'un establiment de l'encarregat en la mesura que l'encarregat està subjecte a obligacions específiques d'acord amb aquest Reglament;

Representant: persona física o jurídica establida a la Unió que, havent sigut designada per escrit pel responsable o l'encarregat del tractament d'acord amb l'article 27 del Reglament, represente el responsable o l'encarregat pel que fa a les seues obligacions respectives en virtut del present Reglament;

Empresa: persona física o jurídica dedicada a una activitat econòmica, independentment de la seua forma jurídica, incloses les societats o associacions que exerceixen 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 en el territori d'un estat membre per a transferències o un conjunt de transferències de dades personals a un responsable o encarregat en un o més països tercers, dins d'un grup empresarial o una unió d'empreses dedicades a una activitat econòmica conjunta;

Autoritat de control: l'autoritat pública independent establida per un estat membre;

Autoritat de control interessada: l'autoritat de control a què afecta el tractament de dades personals perquè el responsable o l'encarregat del tractament està establit en el territori de l'estat membre d'aquella autoritat de control; o els interessats que resideixen en l'estat membre d'aquella 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'aquella autoritat de control;

Tractament transfronterer: el tractament de dades personals realitzat 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 realitzat 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 suposa el projecte de decisió per als drets i llibertats fonamentals dels interessats i, si és el cas, 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]; això és: tot servei prestat normalment a canvi d'una remuneració, a distància, per via electrònica i a petició individual d'un destinatari de serveis. Als efectes d'aquesta definició, s'entén per:

i) «a distància», un servei prestat sense que les parts estiguen presents simultàniament,
ii) «per via electrònica», un servei enviat des de la font i rebut pel destinatari mitjançant equips electrònics de tractament (inclosa la compressió digital) i d'emmagatzematge de dades i que es transmet, canalitza i rep enterament per fils, ràdio, medis òptics o qualsevol altre medi electromagnètic,
iii) «a petició individual d'un destinatari de serveis», un servei prestat mitjançant transmissió de dades a petició individual;

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

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

Altres definicions de màxim interès:

Cessió o comunicació de dades: Tota revelació de dades realitzada a una persona distinta de l'interessat. (Per exemple, amb fins publicitaris o entre empreses ubicades en diferents països.)

Fonts accessibles al públic: Els fitxers la consulta dels quals pot ser realitzada per qualsevol persona, no impedida per una norma limitativa, o sense més exigència que, si és el cas, l'abonament d'una contraprestació. Tenen la consideració de fonts d'accés públic, exclusivament, el cens promocional[6], els repertoris telefònics en els termes previstos per la seua normativa específica i les llistes de persones pertanyents a grups de professionals

[5] En la nostra legislació nacional, és convenient consultar la Llei de Serveis de la Societat de la Informació i Comerç Electrònic.

[6] No s'ha de confondre el cens promocional (disponible per al públic) amb l'electoral ni amb el padró municipal (dades reservades, només amb fins estadístics). El cens promocional només inclouria nom, cognoms i adreça. A més, quant als mitjans de comunicació, noteu que en qualsevol diari, així com la llista de finats inclou nom i cognoms, la llista de naixements és una nota simple amb el nom dels infants (sense cognom).

(sempre que hagen prestat el seu consentiment) que continguen únicament les dades de nom, títol, professió, activitat, grau acadèmic, adreça i indicació de la seua pertinença al grup. Així mateix, tenen el caràcter de fonts d'accés públic els diaris i butlletins oficials i els mèdia.

Drets

Quins drets té el ciutadà? Què indica la llei? Els nostres usuaris, clients, els nostres veïns, nosaltres, veiem com les nostres dades són recollides i posteriorment tractades. I amb aquestes anem nosaltres. El procés recorda a alguns aquestes llegendes que ens parlen d'aborígens que es negaven a ser fotografiats ja que, així, se'ls furtava l'anima. Bé, és possible que l'anima no ens la roben, però sí que ens poden furtar qualsevol rastre de privacitat.

Sobre què hi podem fer, un resum ens el dona el RGPD en el considerant 59, on llegim que s'han de facilitar, incloent-hi els mecanismes necessaris per a això, l'accés a les dades personals i la seua 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 peticiones als interessats..., o justificar per què no les atén. Anem a parlar ara d'aquests drets, i d'altres amb no menys importància. Comencem amb el dret d'accés, per a anar desglossant la resta en epígrafs successius.

Els drets dels ciutadans s'han actualitzat i incrementat. El dret a l'oblit, la portabilitat…, han vingut per a no anar-se'n. Si volem conèixer la norma, hem d'anar als articles 12 a 18 de la Llei 3/2018 i els articles del 15 al 22 del RGPD.

Es tracta de drets que es poden exercir directament o per mitjà de representant, però sempre l'interessat ha de ser informat sobre els mitjans a la seua disposició per a exercir-los. Es fa càrrec de les sol·licituds el responsable o l'encarregat del tractament per compte del responsable. En general, amb lleus excepcions, el seu exercici és gratuït i la càrrega de la prova de la resposta a l'exercici dels drets correspon al responsable.

Per a desplegar-los emprarem unes fitxes amb aquest format:

Nom del dret	Articles de les normes
Breu descripció	
Consideracions	

Dret d'accés de l'interessat:

Accés	13 3/2018; 15 RGPD

L'interessat tindrà dret a obtenir del responsable del tractament confirmació de si s'estan tractant o no dades personals que li concerneixen i, en aquest cas, dret d'accés a les dades personals i a la informació següent: els fins del tractament; les categories de dades personals de què es tracte; els destinataris o les categories de destinataris a què es comunicaren o comunicaran les dades personals, en particular destinataris en tercers o organitzacions internacionals; si és possible, el termini previst de conservació de les dades personals o, si no és possible, els criteris utilitzats per a determinar aquest termini; l'existència del dret a sol·licitar del responsable la rectificació o supressió de dades personals o la limitació del

tractament de dades personals relatives a l'interessat, o a oposar-s'hi; el dret a presentar una reclamació davant d'una autoritat de control; quan les dades personals no s'hagen obtingut de l'interessat, qualsevol informació disponible sobre l'origen i l'existència de decisions automatitzades, inclosa l'elaboració de perfils.

Quan el responsable tracte una gran quantitat de dades de l'afectat i aquest exerceix el seu dret sense especificar a quines dades es refereix, el responsable podrà sol·licitar-li més concreció.

El dret s'entendrà atorgat si el responsable facilita a l'afectat un sistema d'accés remot, directe i segur a les dades que garantisca, de manera permanent, l'accés a la totalitat. La comunicació a l'afectat del mode en què podrà accedir al dit sistema serà suficient per a tenir per atesa la sol·licitud.

Es podrà considerar repetitiu l'exercici del dret d'accés en més d'una ocasió durant el termini de sis mesos, excepte que hi haja causa legítima per a això; en aquest cas, el responsable podrà cobrar un cànon o negar-se a actuar.

Si l'interessat elegeix un mitjà distint al que se li ofereix amb un cost desproporcionat, serà ell qui ha d'assumir l'excés de costos. En aquest cas no es podran al·legar dilacions indegudes.

S'ha de 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).

Dret de rectificació:

Rectificació	14 3/2018; 16 RGPD

L'interessat tindrà dret a obtenir sense dilació indeguda del responsable del tractament la rectificació de les dades personals inexactes que li concerneixen. Tenint en compte els fins del tractament, l'interessat tindrà dret que es completen les dades personals que siguen incompletes, inclusivament mitjançant una declaració addicional.

Haurà d'indicar a quines dades es refereix i la correcció a realitzar.

Haurà d'acompanyar documentació justificativa de la inexactitud o del caràcter incomplet de les dades.

Dret de supressió, anomenat també dret a l'oblit:

Garriga el defineix com cancel·lació de dades personals que ja no són necessàries per a la realització del propòsit concret que en motivà la recollida i tractament. (Garriga Domínguez, 2010)

Supressió (Oblit)	15 3/2018; 17 RGPD

L'interessat tindrà dret a obtenir sense dilació indeguda del responsable del tractament la supressió de les dades personals que li concerneixen, el qual estarà obligat a suprimir sense dilació indeguda les dades personals quan concórrega alguna de les circumstancies següents: les dades personals ja no siguen necessàries en relació amb els fins per als quals foren

recollides o tractades d'altra manera; l'interessat retire el consentiment en què es basa el tractament de conformitat; l'interessat s'opose al tractament i no prevalguen altres motius; les dades personals s'hagen tractat il·lícitament; les dades personals s'hagen de suprimir per al compliment d'una obligació legal establida en el Dret de la Unió o dels estats membres que s'aplique al responsable del tractament; les dades personals s'hagen obtingut en relació amb l'oferta de serveis de la societat de la informació esmentats en l'article 8, apartat 1 (menors).

Quan haja fet públiques les dades personals i estiga obligat a suprimir les dites dades, el responsable del tractament, tenint en compte la tecnologia disponible i el cost de la seua aplicació, adoptarà mesures raonables, incloses mesures tècniques, amb vista a informar els responsables que estiguen tractant les dades personals de la sol·licitud de l'interessat de supressió de qualsevol enllaç a aquestes dades personals, o qualsevol còpia o rèplica d'aquestes.

Quan la supressió derive de l'exercici del dret d'oposició, el responsable podrà conservar les dades amb la finalitat d'impedir tractaments futurs per a fins de màrqueting directe.

S'aprofundeix per a indicar que és particularment pertinent quan el consentiment es va donar sent infant, 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 a Internet. És una ampliació de drets preexistents, de forma que es reforça el respecte de les dades publicades a Internet, de tal manera que el responsable del tractament que haja fet públiques dades personals estiga obligat a indicar als responsables del tractament que estiguen tractant aquestes dades personals que suprimisquen qualsevol enllaç a aquestes, o les còpies o rèpliques d'aquestes dades, cosa que cal fer considerant possibles canvis en la tecnologia.

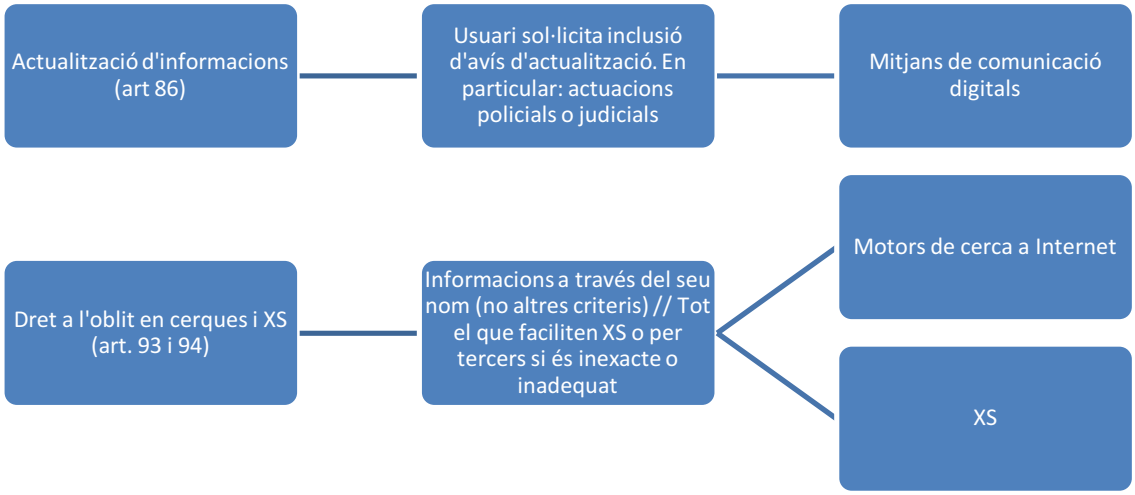
Òbviament, n'hi ha excepcions, entre les quals destaquen les que indiquen que són necessàries per al compliment d'una obligació legal, per al compliment d'una missió realitzada en interès públic (inclòs l'àmbit de la salut), amb fins d'arxiu, investigació científica o històrica o estadístics. D'igual manera, es fa l'excepció pertinent per a quan és necessita la conservació amb vista a l'exercici o defensa de reclamacions.

El precedent clar l'hem de buscar en l'activitat del tribunal europeu en defensa dels ciutadans, cosa que podem particularitzar en la sentència de 13 de maig de 2014 de la Gran Sala del Tribunal de Justícia en el cas del ciutadà espanyol M.C. contra Google, on, 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 efectuada a partir del nom d'una persona vincles a pàgines web, publicades per tercers i que contenen informació relativa a aquesta persona, també en el supòsit que aquest nom o aquesta informació no s'esborren prèviament o simultàniament d'aquestes pàgines web i, si és el cas, tot i que la publicació en les dites pàgines siga en si mateixa lícita (Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, 2014)

Pregunta: Com afectaria això a una hemeroteca virtual històrica, com per exemple la Biblioteca Virtual de Prensa Histórica? (Secretaría de Estado de Cultura)

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



Il·lustració 4. Actualització d'informacions i dret a l'oblit. Elaboració pròpia.

Dret a la limitació del tractament:

Limitació del tractament	16 3/2018; 18 RGPD

L'interessat tindrà dret a obtenir del responsable del tractament la limitació del tractament de les dades quan es complisca alguna de les condicions següents: l'interessat impugne l'exactitud de les dades personals, durant un termini que permeta al responsable verificar-ne l'exactitud; el tractament siga il·lícit i l'interessat s'opose a la supressió de les dades personals i sol·licite al seu lloc la limitació d'ús; el responsable ja no necessite les dades personals per als fins del tractament, però l'interessat les necessite per a la formulació, l'exercici o la defensa de reclamacions; l'interessat s'haja oposat al tractament, mentre es verifica si els motius legítims del responsable prevalen sobre els de l'interessat.

Ha de constar clarament en els sistemes d'informació del responsable.

Seguint el Reglament, s'han d'incloure entre els mètodes per a limitar el tractament de dades personals 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 on la limitació del tractament s'ha de realitzar 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 al seu lloc

la limitació d'ús;
- Quan el responsable ja no necessite les dades personals per als fins del tractament, però l'interessat les necessite per a la formulació, l'exercici o la defensa de reclamacions.

L'interessat serà informat pel responsable abans de l'alçament de la dita limitació.

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

Dret a la portabilitat:

Portabilitat	17 3/2018; 20 RGPD

L'interessat tindrà dret a rebre les dades personals que li incumbeixen, 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 impidisca el responsable a què les haja facilitades, quan: el tractament està basat en el consentiment o en un contracte i el tractament s'efectua per mitjans automatitzats.

L'interessat tindrà dret que les dades personals es transmeten directament de responsable a responsable quan siga tècnicament possible.

És un dret que pot ser molt útil en canviar de companyia de subministres (telèfon, per exemple) o de treball. Verbigràcia, en canviar de companyia de telèfons, l'interessat només ha de demanar la portabilitat, i la companyia que rep aquesta petició és l'encarregada dels tràmits de baixa de la línia anterior.

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

Dret d'oposició

Oposició	18 3/2018; 21 i 22 RGPD

L'interessat tindrà dret a oposar-se en qualsevol moment, per motius relacionats amb la seua situació particular, que dades personals que li concernisquen siguen objecte d'un tractament, inclosa l'elaboració de perfils sobre la base de les dites disposicions. El responsable del tractament deixarà de tractar les dades personals, tret que acredite motius legítims imperiosos per al tractament que prevalguen sobre els interessos, els drets i les llibertats de l'interessat, o per a la formulació, l'exercici o la defensa de reclamacions. Quan el tractament de dades personals tinga per objecte el màrqueting directe, l'interessat tindrà dret a oposar-se a cada moment al tractament de les dades personals que li concernisquen, inclosa l'elaboració de perfils en la mesura que estiga relacionada amb el màrqueting esmentat.

Quan les dades personals es tracten amb fins d'investigació científica o històrica o fins estadístics, l'interessat tindrà dret, per motius relacionats amb la seua situació particular, a oposar-se al tractament de dades personals que li concernisquen, tret que siga necessari per al compliment d'una missió realitzada per raons d'interès públic.

Qualsevol interessat tindrà dret a no ser objecte d'una decisió basada únicament en el tractament automatitzat, inclosa l'elaboració de perfils, que produïsca efectes jurídics en ell o l'afecte significativament de manera semblant.

Decisions individuals automatitzades (elaboració de perfils):

Parlem ara d'un dret que no sol ser inclòs en les llistes, però que entenem té molt d'interès per a l'informàtic (recollit en l'article 22 del RGPD), el que té l'usuari a no ser objecte d'una decisió que avalue aspectes personals, i que aquesta 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 no fer-ho) aspectes personals relatius a una persona física, per a analitzar o predir aspectes relacionats amb el rendiment en el treball, la situació econòmica, la salut, les preferències o interessos personals, la fiabilitat o el comportament, la situació o els moviments de l'interessat... (Vegeu per exemple la pel·lícula-documental *Siclo* de Michael Moore (Moore , 2007)[7]). D'altra banda, si es permeten les decisions basades en aquest tractament, inclosa l'elaboració de perfils, si l'autoritza expressament el Dret de la Unió o dels estats membres, per exemple, per al control i 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 que l'interessat haja donat el seu consentiment explícit. Les garanties d'aquest tractament de qualsevol forma s'ha de cenyir a les garanties apropiades (donar informació específica a l'interessat; dret a obtenir intervenció humana; dret a expressar el seu 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, i impedir 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?

Hem vist un conjunt molt important de drets, però aquests no signifiquen una barra lliure perquè els usuaris els exercisquen a manera de castic cap a les organitzacions. Hem vist com s'al·ludeix a pagament d'un cànon quan les peticions són repetitives, per exemple. Però n'hi ha més limitacions, que es poden trobar en el RGPD, en l'article 23 i en el seu considerant 19. Els estats membres poden encomanar a les autoritats competents (Vegeu la Directiva (UE) 2016/680) (Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, 2016) funcions que no es porten a cap necessàriament amb fins de prevenció, investigació, detecció o

[7] Es tracta d'una visió molt crítica sobre el sistema de salut dels Estats Units, en concret sobre les companyies sanitàries privades respecte a un sistema de salut públic com el que gaudim en alguns països europeus.

enjudiciament d'infraccions penals o execució de sancions penals, inclosa la protecció enfront de les amenaces a la seguretat pública i la seua prevenció, que indica expressament que els estats membres puguen, en condicions específiques, limitar d'acord amb el Dret determinades obligacions i drets sempre que la dita limitació siga una mesura necessària i proporcionada en una societat democràtica per a protegir interessos específics importants.

Això implica que s'han de respectar essencialment els drets i llibertats fonamentals, a pesar de 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 deontològiques en les professions regulades; la protecció de l'interessat o dels drets i llibertats d'altres.

Plantejament obert: si ens fixem, en incloure's la prevenció d'infraccions penals, s'autoritzen expressament les aplicacions de *precrim*, que permeten anticipar sobre quines zones o quins individus cal reforçar la vigilància?

Articles de màxim interès per a entendre els drets:

Article 12 de la Llei 3/2018. Disposicions generals sobre exercici dels drets.

Article 13 de la Llei 3/2018. Dret d'accés.

Article 14 de la Llei 3/2018. Dret de rectificació.

Article 15 de la Llei 3/2018. Dret de supressió.

Article 16 de la Llei 3/2018. Dret a la limitació del tractament.

Article 17 de la Llei 3/2018. Dret a la portabilitat.

Article 18 de la Llei 3/2018. Dret d'oposició.

RGPD. Article 15. Dret d'accés de l'interessat.

RGPD. Article 16. Dret de rectificació.

RGPD. Article 17. Dret de supressió («el dret a l'oblit»).

RGPD. Article 18. Dret a la limitació del tractament.

RGPD. Article 19. Obligació de notificació relativa a la rectificació o supressió de dades personals o la limitació del tractament.

RGPD. Article 20. Dret a la portabilitat de les dades.

RGPD. Article 21. Dret d'oposició.

RGPD. Article 22. Decisions individuals automatitzades, inclosa l'elaboració de perfils.

Les autoritats de control: l'Agencia Española de Protección de Datos (AEPD) i agències autonòmiques

És de màxim interès conèixer els *vigilants de la llei*. A Espanya, parlem respecte a això de l'AEPD i les agències autonòmiques (a França de la CNIL, Commission nationale de l'informatique et des libertés, a Itàlia de la Garante per la protezione dei dati personali). No són entitats de nova creació, ja porten molts lustres entre nosaltres, però alguns canvis han experimentat. Per a deixar clar el marc en què es mouen, hauríem de recórrer a la Llei 3/2018, als articles 44 a 62 i disposicions addicionals vintena i transitòria primera, i en el RGPD, als articles 51 a 67.

De fet, l'Estatut Jurídic actual continua en vigor de manera un poc provisional, ja que la llei indica que seguirà vigent en la part que no s'opose al que estableix la llei orgànica. D'igual manera, s'indica que la nova regulació relativa a l'adjunt de la Presidència de l'Agencia i al Consell Consultiu de l'Agencia no s'aplicarà fins que no expire el mandat del director de l'Agencia a l'entrada en vigor de la llei orgànica.

I en què s'ha d'ocupar l'AEPD? (Funcions de l'AEPD)

- Investigació (en cas de vulneració de la normativa i mitjançant auditories preventives). Administracions públiques i particulars estan obligats a proporcionar informes, antecedents i justificants.
- Regulació: Dictant disposicions que fixen els criteris d'actuació: Circulars que són de compliment obligatori una vegada publicades en el BOE.
- Acció exterior: funcions relacionades amb l'acció exterior de l'Estat en matèria de protecció de dades. Ídem a les comunitats autònomes, a través de les autoritats autonòmiques.

La confusió pot venir de la coexistència en un mateix territori de diverses autoritats de control. Se succeeixen preguntes com ara: si es dona una violació de la llei en alguna matèria que siga competència autonòmica, pot l'AEPD requerir a les agències autonòmiques? La resposta és elemental: sí. Sobre aquestes, deixem clar que el seu àmbit d'actuació queda limitat als fitxers de titularitat pública declarats per les administracions autonòmiques i locals de les comunitats autònomes respectives.

Comencem deixant clar què és l'AEPD: es tracta d'un ens de Dret Públic, amb personalitat jurídica pròpia i plena capacitat pública i privada, que actua amb plena independència de les administracions públiques en l'exercici de les seues funcions (que no vol dir que siga totalment independent, ja que està sotmesa al Tribunal de Cuentas). La seua finalitat principal és vetlar pel compliment de la legislació sobre protecció de dades personals i controlar-ne l'aplicació.

I recordem que és l'espanyola. Pensem que es pot donar el cas d'un ciutadà espanyol que tinga un problema amb una empresa francesa. O un ciutadà italià amb un problema amb una

empresa espanyola. Què succeeix? Quina agència atén? Quina autoritat hem de considerar la principal?

El fet que una autoritat de control puga o no actuar com a autoritat principal, segons es tracten assumptes locals o quan afecta interessats d'aquest únic estat membre, provoca la necessària coordinació entre autoritats de control que ha d'informar sense dilació i decidir si s'ha d'emprar el «mecanisme de finestreta única[8]» o si ho ha de tractar localment l'autoritat de control que l'haja informat (Considerant 127).

Recordem que en l'apartat de definicions, dèiem que **Autoritat de control** és l'autoritat pública independent establida per un estat membre d'acord amb el que disposa l'article 51 del Reglament. Convé que sapiem ara què diu aquest article 51.

Cada estat membre establirà 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. Aquestes autoritats de control cooperaran entre si. És possible que hi haja diverses autoritats de control en un estat membre; una d'aquestes serà la que represente les dites 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, anem a veure ara uns quants aspectes d'interès. Comencem per la seua composició: Quins són els membres de l'autoritat de control? (Article 53)

Els membres de les autoritats de control han de ser nomenats mitjançant un procediment transparent, que deixa que cada país de la Unió decidisca si seran pel seu parlament, govern o cap d'estat, o un organisme independent encarregat del nomenament. En tot cas, cada membre posseirà la titulació, experiència i aptituds, en l'àmbit de la protecció de dades personals, necessaris per al compliment de les seues funcions i l'exercici dels seus poders. Serà destituït abans del fi de mandat únicament en cas de conducta irregular greu o si deixa de complir les condicions exigides en l'exercici de les seues funcions.
Cada estat membre de la Unió establirà respecte als seus 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, tret del primer nomenament posterior al 24 de maig de 2016;
- el caràcter renovable o no del mandat del membre o els membres de cada autoritat de control i, si és el cas, el nombre de vegades que es podrà renovar;
- les condicions, prohibicions relatives a accions, ocupacions i prestacions incompatibles amb el càrrec durant el mandat i després d'aquest i les normes que regeixen el cessament en l'ocupació.

[8] 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 d'interlocutora. Això no suposa que els ciutadans s'han de relacionar amb diverses autoritats o amb autoritats distintes de la de l'estat on resideix. Sempre poden plantejar les reclamacions o denúncies a la pròpia autoritat nacional.

L'autoritat de control que tenim a Espanya és l'Agencia Española de Protección de Datos, que definíem com un Ens de Dret Públic, que actua amb plena independència de les administracions públiques en l'exercici de les seues funcions. 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).

Dèiem que la seua finalitat principal és vetlar pel compliment de la legislació sobre protecció de dades personals i controlar-ne l'aplicació. Per al compliment d'aquesta missió, l'Agencia realitza campanyes de divulgació per a una millor defensa dels drets dels ciutadans. L'AEPD porta a cap les seues potestats d'investigació fonamentalment a instància dels ciutadans, tot i que també està facultada per a actuar d'ofici.

L'AEPD, creada el 1993, és l'organisme públic encarregat de vetlar pel compliment de 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.

Recordem que les agències de protecció de dades de caràcter autonòmic (Catalunya i País Basc) tenen un àmbit d'actuació limitat als fitxers de titularitat pública declarats per les administracions autonòmiques i locals de les seues respectives comunitats autònomes.

Els membres i el personal de cada autoritat de control estaran subjectes al deure de secret professional, tant durant el seu mandat com després d'aquest.

Cal destacar (Article 55) que les autoritats de control no seran competents per a controlar les operacions de tractament efectuades pels tribunals en l'exercici de la seua funció judicial.

L'autoritat de control inclou en els seues competències (Article 56): tractar les reclamacions presentades o infraccions del Reglament i, si 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 pretén fer un tractament transfronterer de dades, actuar com a autoritat de control principal.

Algunes de les seues funcions: (*Article57)*

Pel que fa a l'interessat:

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

Pel que fa a la societat en general:

- controlar l'aplicació del Reglament i fer-ho aplicar;
- promoure la sensibilització del públic i la seua comprensió dels riscos, normes, garanties i drets en relació amb el tractament. Amb especial atenció als infants;
- assessorar el parlament, 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;

Pel que fa al responsable i l'encarregat del tractament:

- promoure la sensibilització dels responsables i encarregats del tractament sobre les seues obligacions;
- elaborar i mantenir una llista relativa al requisit de l'avaluació d'impacte referent a la protecció de dades;
- oferir assessorament sobre les operacions de tractament;
- encoratjar a 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

Pel que fa a altres autoritats de control i funció investigadora:

- cooperar amb altres autoritats de control i prestar assistència mútua;
- portar a cap investigacions en particular basant-se en informació rebuda d'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 podrà 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)

Pel que fa al responsable i a l'encarregat del tractament i, si és el cas, al representant del responsable o de l'encarregat, pot ordenar-los que faciliten qualsevol informació que requerisca per a l'exercici 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 funciones i notificar al responsable o a l'encarregat del tractament les presumptes infraccions; per a això, pot portar a cap investigacions en forma d'auditories de protecció de dades i dur a terme una revisió dels certificats expedits.

Una vegada es detecta un fet digne de sanció, es pot sancionar qualsevol responsable o encarregat del tractament mitjançant un advertiment o amb una advertència i ordenar al responsable o encarregat del tractament que atenguen les sol·licituds d'exercici dels drets de l'interessat, i ordenar-los que les operacions de tractament s'ajusten a les disposicions del Reglament, quan pertoque, d'una determinada manera 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.

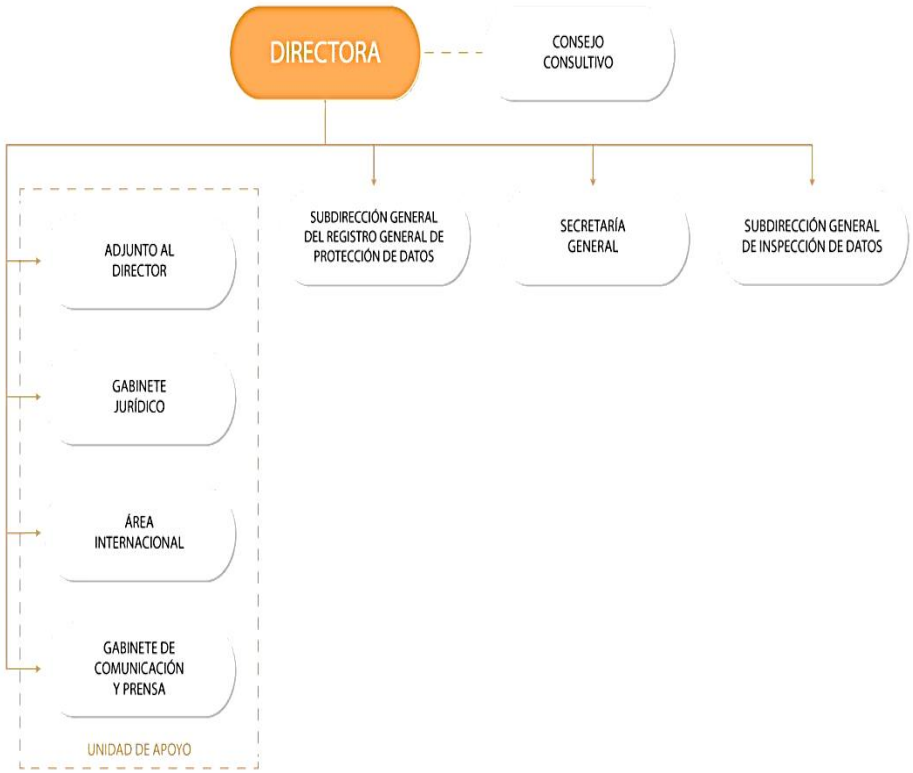
Pot imposar una limitació temporal o definitiva del tractament, inclosa la prohibició, retirar un certificat, imposar una multa administrativa i ordenar la suspensió dels fluxos de dades cap a un destinatari situat en un tercer país.

Pel que fa a l'assessorament i informació, pot assessorar el responsable del tractament conforme al procediment de consulta prèvia, emetre, per iniciativa pròpia o després de la 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.

És important ressenyar la vinculació de les autoritats de control amb els codis de conducta. A això tornarem en aquest mateix tema.

Agencia Española de Protección de Datos

Tot i que ja hem presentat l'AEPD, parlarem un poc de la seua estructura i funcionament. Comencem veient un organigrama de l'Agencia Española de Protección de Datos:



Il·lustració 5. Organigrama de l'AEPD. Font: (Agencia Española de Protección de Datos, 2018)

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

El Registre General de Protecció de Dades:

Quin paper té en aquesta qüestió el Registre General? Sense ànim exhaustiu, en aquesta part de l'AEPD:

- Es promocionen, registren i publiquen els codis de conducta i tramita i valora les sol·licituds d'aprovació.
- S'elaboren els criteris per a l'acreditació dels organismes de supervisió dels codis de conducta i se'n tramiten i valoren l'acreditació i revocació.

- Es promocionen els certificats, segells i marques en protecció de dades. S'elaboren els criteris per a l'acreditació dels organismes de certificació i es realitza el control dels certificats expedits i la seua revisió periòdica.
- S'encarreguen de l'elaboració i tramitació de 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.
- S'elaboren materials d'ajuda a responsables i encarregats en el compliment de la normativa de protecció de dades.
- S'atenen les consultes plantejades per responsables, encarregats i delegats de protecció. També s'atenen les consultes presentades pels ciutadans sobre exercici dels seus drets i presentació de reclamacions.
- Es fa càrrec de les tasques relatives a la transparència exigides a l'Agencia.

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 ONG.

Fixem-nos de nou en els punts de contacte entre AEPD i codis de conducta.

La inspecció de dades

D'igual manera, sense ànim de completesa, intentem destacar-ne les principals funcions:

- Supervisió permanent del compliment de la normativa en matèria de protecció de dades pels responsables i encarregats dels tractaments, incloent-hi l'atenció als ciutadans en l'exercici dels seus drets d'accés, rectificació, oposició, supressió, oposició a decisions automatitzades, limitació al tractament i portabilitat.
    - Per a efectuar aquesta supervisió, al seu torn, es realitza l'anàlisi de les reclamacions per incidències concretes, per a determinar si les vulneracions de la normativa s'han produït per errors puntuals o bé es deuen a causes sistèmiques; en aquest cas, l'Agencia investigarà l'origen del problema: això és, el sistema de gestió de dades del responsable o encarregat del tractament.
- Realització d'investigacions en forma d'auditories de protecció de dades, que manté diàleg permanent amb els delegats de protecció de dades, als efectes de resoldre les reclamacions que presenten els afectats.
- Comprovació del compliment dels codis de conducta.

Les 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 d'aquests. Una de les seues manifestacions és l'exercici de la potestat sancionadora.

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

Però té altres labors, entre les quals destaca la necessària cooperació amb altres autoritats de control; proposar d'imposar una limitació temporal o definitiva del tractament, inclosa la seua prohibició, o proposar ordenar la suspensió de fluxos de dades cap un destinatari situat en un tercer país o cap a una organització internacional.

Director/a de l'AEPD

El director o la directora exerceix la representació de l'Agencia i els seus actes es consideren actes propis de l'Agencia. Les seues resolucions posen fi a la via administrativa i són recurribles davant la Sala Contenciosa de l'Audiencia Nacional.

Efectua el nomenament el Govern mitjançant reial decret entre els que componen 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 ple sotmetiment al Dret. Exerceix les seues funcions amb dedicació exclusiva, plena independència i total objectivitat.

De les seues funcions, destaquem:

- Dictar les resolucions i instruccions que requerisca l'exercici de les funcions de l'Agencia.
- La coordinació amb les autoritats autonòmiques.
- La representació de l'Agencia en l'àmbit internacional.
- Funcions de gestió (adjudicar i formalitzar els contractes; aprovar despeses i ordenar pagaments...).

El treball del professional de la informació

Parlarem en aquest apartat de les tasques que ha de portar a cap el professional, en alguns dels rols més destacats, i ens centrarem en la figura de l'encarregat del tractament, però sense oblidar les del responsable o el delegat de dades...

Hi ha elements que s'han de portar a cap amb la màxima diligència, com ara el registre de les activitats de tractament, l'avaluació d'impacte, l'atenció als drets dels seus usuaris..., anirem detallant els més importants.

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

I què implica aquesta responsabilitat activa? Bàsicament, que les empreses han d'adoptar mesures que asseguren raonablement que estan en condicions de complir amb els principis, drets i garanties, amb un full de ruta prolix que inclouria[9]:

- Protecció de dades des del disseny.
- Protecció de dades per defecte.
- Mesures de seguretat.
- Manteniment d'un registre de tractaments
- Realització d'avaluacions d'impacte sobre la protecció de dades.
- Nomenament d'un delegat de protecció de dades.

[9] Un pas excel·lent per a no perdre's és atendre les recomanacions de l'AEPD. Per exemple, seguir el "Listado de cumplimiento normativo" (AEPD, 2018).

- Notificació de violacions de la seguretat de les dades.
- Promoció de codis de conducta i esquemes de certificació.

Abans de començar, el professional s'ha de plantejar un seguit de preguntes com ara: es poden generar amb el tractament situacions de discriminació, usurpació d'identitat o frau, pèrdues financeres, dany…? Es pot privar els afectats dels seus drets i llibertats? Es treballa amb categories especials[10] de dades o dades relacionades amb la comissió d'infraccions administratives? Es creen perfils? Sobre economia, salut…? Es tracta de dades de grups d'afectats vulnerables?[11] Es tracta d'un tractament massiu? Es donarà una transferència, amb caràcter habitual, a tercers estats o organitzacions internacionals sense un nivell adequat de protecció?

Això és… s'ha de posar en el pitjor dels casos. Ha de preveure, i per a això és molt recomanable que, *a priori*, considere els codis de conducta i estàndards definits.

Actuacions del responsable i de l'encarregat del tractament

Hi ha dos elements de molta consideració: les mesures de responsabilitat activa i l'avaluació d'impacte. Podem tenir una relació completa en l'article 28 de la Llei 3/18 i en els 24 i 25 del RGPD

A manera de resum, veiem quins serien els tractaments de més risc que impliquen considerar mesures i realitzar avaluacions d'impacte. Hem de plantejar-nos...

Es poden generar amb el tractament situacions de discriminació, usurpació d'identitat o frau, pèrdues financeres, dany per a la reputació, pèrdua de confidencialitat de dades subjectes al secret professional, reversió no autoritzada de la pseudonimització o qualsevol altre perjudici econòmic, moral o social significatiu per als afectats?

Pot el tractament privar els afectats dels seus drets i llibertats o impedir-los el control sobre les seues dades personals?

Es tracta d'un tractament no merament accessori de les categories especials de dades o de dades relacionades amb la comissió d'infraccions administratives?

Implica el tractament una avaluació d'aspectes personals dels afectats a fi de crear o utilitzar-ne perfils personals, en particular mitjançant l'anàlisi o la predicció d'aspectes referits al seu rendiment en el treball, situació econòmica, salut, preferències o interessos personals, fiabilitat o comportament, solvència financera, localització o moviments?

Es tracta de dades de grups d'afectats en situació d'especial vulnerabilitat, en particular, menors d'edat i persones amb discapacitat?

Es tracta d'un tractament massiu que implique un gran nombre d'afectats o la recollida d'una gran quantitat de dades personals?

[10] Dades genètiques, dades biomètriques, dades relatives a la salut…

[11] Menors d'edat i persones amb discapacitat…

Les dades personals seran objecte de transferència, amb caràcter habitual, a tercers estats o organitzacions internacionals respecte de les quals no s'haguera declarat un nivell adequat de protecció?

A més de tot l'anterior, cal considerar a judici del responsable o de l'encarregat altres factors amb rellevància, sobretot els previstos en codis de conducta i estàndards definits.

Aquest punt es desplegarà en annexos.

Registre d'activitats de tractament

Una de les tasques en què el professional ha de posar més interès, ja que es tracta d'un fet que es produeix en el seu dia a dia laboral, és el del registre de les activitats del tractament. En la Llei 3/2018 podem trobar en l'article 31 la regulació corresponent, així com en l'article 30 del RGPD.

Aquest registre es pot organitzar mitjançant conjunts estructurats de dades, i ha d'especificar les activitats de tractament portades a cap i les altres circumstancies que el RGPD estableix. Qualsevol canvi en el contingut d'aquest registre s'ha de comunicar al DPD, si n'hi ha. L'inventari de les activitats de tractament ha de ser públic i accessible per mitjans electrònics i incloure:

- el nom i les dades de contacte del responsable i, si és el cas, del corresponsable, del representant del responsable i del delegat de protecció de dades;
- els fins del tractament;
- una descripció de les categories d'interessats i de les categories de dades personals;
- les categories de destinataris als quals es comunicaren o comunicaran les dades personals, inclosos els destinataris en tercers països o organitzacions internacionals;
- si és el cas, les transferències de dades personals a un tercer país o una organització internacional, inclosa la identificació del dit tercer país o organització internacional;
- si és possible, els terminis previstos per a la supressió de les diferents categories de dades i una descripció general de les mesures tècniques i organitzatives de seguretat.

A més, cada encarregat portarà un registre de totes les categories d'activitats de tractament efectuades per compte d'un responsable que ha de contenir:

- Nom i dades de contacte de l'encarregat o encarregats i de cada responsable per compte del qual actua l'encarregat i, si és el cas, del representant del responsable o de l'encarregat i del delegat de protecció de dades;
- Categories de tractaments efectuats per compte de cada responsable;
- Si n'hi ha, transferències de dades personals a un tercer país;
- Quan siga possible, una descripció general de les mesures tècniques i organitzatives de seguretat.

Aquests registres, d'encarregat i responsable, constaran per escrit i es posaran a disposició de l'autoritat de control que ho sol·licite. Cal indicar que no són aplicables a cap empresa ni organització que empre menys de 250 persones, tret que el tractament que realitze puga

suposar 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 que hi havia en la LOPD, 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.

El registre d'activitats de tractament serveix com a primer element per a valorar el compromís del responsable i l'encarregat amb els requisits legals. S'hi ressenyen tant els fitxers que s'empren com les mesures de seguretat usades.

Perfils i informació a l'afectat: transparència

Les capacitats de càlcul dels processadors permeten jugar molt amb les dades i elaborar perfils cada vegada més complexos del nostre comportament. A això no és cega la llei, que obliga a informar l'afectat sobre l'existència d'aquests perfils, que es pot veure en la Llei 3/2018 en l'article 11 i en particular en el RGPD, en els articles 12, 13 i 14, amb especial atenció als perfils en l'article 22.

Cal distingir dues possibilitats: que l'interessat donara les seues dades directament o que no procedisquen de forma directa d'ell.

En tot cas, s'han de facilitar: la identitat i les dades de contacte del responsable i, si és el cas, del seu representant, incloent-hi una adreça electrònica o un altre mitjà similar perquè es puguen posar en contacte. Si hi ha DPD, també les seues dades de contacte; els fins del tractament a què es destinen les dades personals i la base jurídica del tractament, així com els interessos legítims del responsable o d'un tercer per a efectuar-lo; els destinataris o les categories de destinataris de les dades personals, i si es tracta de dades no donades directament pels afectats, les fonts de què procedeixen i, si és el cas, informar sobre la intenció del responsable de transferir dades personals a un tercer país o organització internacional.

Ha de quedar clar a l'afectat la possibilitat d'exercir els seus drets, entre els quals, destaca no ser objecte d'una decisió basada únicament en el tractament automatitzat, inclosa l'elaboració de perfils, que produïsca efectes jurídics en ell o l'afecte significativament de manera similar.

També cal facilitar el termini durant el qual es conservaran les dades personals o, quan no siga possible, els criteris utilitzats per a determinar aquest termini; l'existència de decisions automatitzades, inclosa l'elaboració de perfils, i quan el responsable del tractament projecte el tractament ulterior de dades personals per a un fi que no siga aquell per al qual es recolliren, proporcionarà a l'interessat, amb anterioritat al dit tractament, informació sobre aquest;

És important informar sobre el dret a sol·licitar al responsable del tractament l'accés, rectificació o supressió, limitació, oposició i portabilitat de les dades i el dret a presentar una reclamació davant una autoritat de control.

Si l'interessat és qui ens facilita les seues dades, hem d'indicar si la comunicació d'aquestes és un requisit legal o contractual o un requisit necessari per a subscriure un contracte. Si les dades no venen directament de l'interessat, cal afegir la font de què procedeixen les dades personals i, si és el cas, si procedeixen de fonts d'accés públic.

El termini indicat és, a tot tardar, un mes des de l'obtenció de les dades personals, per a comunicar si aquestes s'empraran per a la comunicació amb l'interessat i, si està previst comunicar-les a un altre destinatari, com més tard en el moment que les dades personals siguen comunicades per primera vegada. Però això no és aplicable si l'interessat ja disposa de la informació o comunicar aquesta suposa un esforç desproporcionat, sobretot quan es tracte de tractament amb fins d'arxivament en interès públic (investigació científica, històrica o fins estadístics); o bé si l'obtenció o comunicació està expressament establida pel Dret de la Unió o dels estats membres, o quan les dades personals han de seguir tenint caràcter confidencial sobre la base d'una obligació de secret professional regulada pel Dret de la Unió o dels estats membres.

I com s'han d'oferir aquestes informacions? En un format estructurat, d'ús comú, de lectura mecànica i interoperable[12]. El dret de l'interessat a transmetre o rebre dades personals que el concerneixen 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: Això no ha d'implicar la supressió de les dades personals concernents a l'interessat que aquest 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.

Articles de màxim interès per a entendre els perfils:

Article 11 de la Llei 3/2018. Transparència i informació a l'afectat.

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

RGPD. Article 13. Informació que s'ha de facilitar quan les dades personals s'obtenen de l'interessat.

RGPD. Article 14. Informació que s'ha de facilitar quan les dades personals no s'han obtingut de l'interessat.

RGPD. Article 22. Decisions individuals automatitzades, inclosa l'elaboració de perfils.

Seguretat del tractament

El Reglament obliga que, considerant l'estat de la tècnica, els costos d'aplicació i la naturalesa, l'abast, el context i els fins 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

[12] Per això, des dels estats s'encoratja els responsables a crear formats interoperables que permeten la portabilitat de dades.

tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat al risc[13]. (Article 32)

Aquestes mesures passen per emprar:

- la pseudonimització i el xifratge 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 forma 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 serien 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 dites dades.

Busquem evitar danys i perjudicis físics, materials o immaterials, en particular en els casos en què el tractament puga donar lloc, per exemple, a problemes de discriminació, usurpació d'identitat o frau, pèrdues financeres, dany per a la reputació…

Cal recordar en aquest punt que el Reglament preveu la protecció de dades des del disseny i, per defecte, en l'article 25.

I si es produeix una violació de la seguretat de les dades personals? Aquest és un dels moments crítics per al professional. A més d'indicar-lo el sentit comú, la norma adverteix de la necessària notificació, no solament a l'interessat (Article 34), sinó també a l'autoritat de control (Article 33), amb uns terminis molt breus.

Què ha de contenir cada notificació? Abans de res, precisem que l'AEPD ofereix un suport fantàstic a aquest respecte, amb la seua *Guía para la gestión y notificación de brechas de seguridad* (AEPD & INCIBE, 2017).

Amb vista a l'autoritat de control, ha de constar:

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 afectades;
2. nom i dades de contacte del delegat de protecció de dades o d'altre punt de contacte en què es puga obtenir més informació;
3. descripció de les possibles conseqüències de la violació de la seguretat de les dades personals;
4. descripció de les mesures adoptades o proposades pel responsable del tractament per

[13] És molt difícil avaluar el risc. Posem dos exemples de ciberatacs amb robatori de dades personals: D'una banda, un atac d'Anonymous on s'emportaren més de 200GB d'informació de la base de dades de Stratfor Global, companyia especialitzada en seguretat, amb informació dels seus 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? La pregunta important ací és "què podria passar". I la resposta és esgarrifosa. Enfront d'aquest cas de dimensions quasi globals, ens trobem uns altres més d'anar per casa, com el 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 podem evitar-ho?

a posar remei a la violació de la seguretat de les dades personals, incloent-hi, si cal, les mesures adoptades per a mitigar els possibles efectes negatius.

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

Qualsevol violació de la seguretat la documentarà el responsable del tractament.

I el secret professional?

Els estats membres podran 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 calga. Aquestes normes només s'aplicaran a les dades personals rebudes en ocasió d'una activitat coberta per l'obligació de secret. (Article 90)

Procurant un equilibri entre el tècnicament possible en cada moment, i els riscos que comporta el tractament de dades, el responsable del tractament aplicarà, tant en el moment de determinar els mitjans de tractament com en el moment del mateix 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 necessàries per a cadascun dels fins específics del tractament, fet que s'ha d'entendre tant pel que fa a l'extensió del seu tractament, com al termini de conservació i accessibilitat. Això és el que entenem per Protecció de dades des del disseny i per defecte.** (Article 25)[14]

En els tractaments que no requereixen identificació d'un interessat pel responsable, aquest no estarà obligat a mantenir, obtenir o tractar informació addicional amb vista a identificar l'interessat amb l'única finalitat de complir el Reglament. Si és capaç de demostrar que no està en condicions d'identificar l'interessat, li informarà si és possible. (Article 11)

Un assumpte espinós per a qualsevol professional és la confidencialitat, que sovint es confon amb el secret professional. En el cas de la protecció de dades, a més, les normes en parlen expressament. Els articles d'interès són els mateixos que per al consentiment.

[14]Aquest principi de privacitat des del disseny (art. 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, en què l'usuari ha de ser el que els obri a altres.

La primera pregunta seria, doncs, qui està subjecte al deure de confidencialitat? La resposta és molt àmplia: responsables i encarregats del tractament, així com els que intervenen en qualsevol fase d'aquest.

La segona i més important és: fins a quan es manté el deure de confidencialitat? Aquest deure, complementari al de secret professional quan la relació professional està en actiu, es manté tot i que haguera finalitzat la relació de l'obligació a guardar secret amb el responsable o encarregat del tractament de les dades.

Com i quan es realitza una avaluació d'impacte relativa a la protecció de dades?

Sobre aquest punt hi ha unes directrius que detallen de manera conscienciosa què fer. Es tracta de la WP 248 (Grupo "Protección de datos" del artículo 29, 2017). El punt fonamental a repassar en el RGPD és l'article 35.

Els tractaments de dades empren tècniques canviants en el temps. Sovint, ens trobem amb problemes, amb forats de seguretat, que resulten absolutament inesperats. D'altres, hi ha indicis que ens avisen per on poden venir els problemes.

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

El resultat de l'avaluació s'ha de tenir en compte quan es decidisquen les mesures adequades que s'han de prendre a fi de demostrar que el tractament de les dades personals és correcte (Considerant 84). Es realitzarà abans del tractament, amb l'assessorament del delegat de protecció de dades, si n'hi ha.

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

Quines operacions són les que necessiten d'una avaluació d'impacte? Quines no? L'autoritat de control (Agencia Española de Protección de Datos, 2018) té entre les seues funcions informar-ne. Però tenim una eina fabulosa en les directrius del Grup 29 (Grupo "Protección de datos" del artículo 29, 2017).

En el document de l'Agencia (AEPD, 2017) ens trobem amb aquest gràfic que és molt clarificador respecte del possible flux de treball que un responsable ha de seguir.

Il·lustració 6. Full de ruta a seguir per un responsable del tractament. (AEPD, 2017)

L'avaluació ha d'incloure com a mínim:

1. una descripció sistemàtica de les operacions de tractament previstes i dels fins del tractament, inclusivament l'interès legítim perseguit pel responsable del tractament;
2. una avaluació de la necessitat i la proporcionalitat de les operacions de tractament respecte a la seua finalitat;
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 garantisqueen la protecció de dades personals.

El compliment dels codis de conducta pels responsables o encarregats corresponents es tindrà degudament en compte en avaluar les repercussions de les operacions de tractament, en particular als efectes de l'avaluació d'impacte relativa a la protecció de dades.

Si cal, el responsable examinarà 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).

El responsable facilitarà a l'autoritat de control l'avaluació d'impacte relativa a la protecció de dades i informarà l'autoritat de control sobre les responsabilitats respectives del responsable, els corresponsables i els encarregats, així com dels fins i mitjans del tractament previstos i les mesures i garanties establides. Si n'hi ha, també facilitarà 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)

És de molt d'interès l'aplicació de l'AEPD per a realitzar avaluacions d'impacte: https://gestiona.aepd.es/

Com ha d'actuar el professional davant de la transparència?

Hem parlat de l'aparent incompatibilitat d'algunes lleis. Hem destacat ja com la protecció de dades i la llibertat d'expressió semblen xocar i avançàrem un poc 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 aquests no seran els nostres secrets, sinó els dels propietaris de les dades.

Ara, per a reblar el clau: hem de ser transparents en el nostre treball. Hem de fer veure com impedim que es veja el que la llei impedeix veure. Aquest embarbussament té resposta en l'article 12 del Reglament. I és molt interessant per estar íntimament lligat al punt que veurem a continuació, un dels que desperta més preocupació entre els professionals: el consentiment.

L'interessat ha de conèixer l'existència de l'operació de tractament i els seus fins. El responsable del tractament ha de facilitar a l'interessat tota la informació complementària que siga necessària per a garantir un tractament lleial i transparent, i considerar circumstancies i context. Així mateix, ha d'informar l'interessat sobre l'existència de l'elaboració de perfils i de les conseqüències de la dita elaboració. Si les dades personals s'obtenen dels interessats, també se'ls ha d'informar sobre si estan obligats a facilitar-los i de les conseqüències en cas que no ho feren. Aquesta informació es pot transmetre en combinació amb unes icones normalitzades que oferisquen, de forma fàcilment visible, intel·ligible i clarament llegible, una adequada visió de conjunt 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 infant.

Sempre hem de 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 forma verbal, la resposta pot donar-se d'aquesta forma, sempre que estiga suficientment acreditada la identitat del peticionari. Es pot sol·licitar que es facilite la informació addicional necessària per a confirmar la identitat de l'interessat, fet lògic, per a evitar donar 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, tret que l'interessat sol·licite que es facilite d'una altra manera. La informació facilitada així com tota comunicació i qualsevol actuació seran a títol gratuït.

Quant als terminis, en un mes s'ha de donar complida resposta i, si per raons de complexitat o d'elevat nombre de sol·licituds no és possible, es pot prorrogar uns altres dos mesos, informar l'interessat sobre la dita pròrroga en el termini d'un mes a partir de la recepció de la sol·licitud, i indicar els motius de la dilació. Si no dona curs a la sol·licitud i no informa sobre les raons de la 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 (p. e. pel seu 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 realitzar l'actuació sol·licitada o negar-se a actuar respecte de la sol·licitud. En tot cas, el responsable del tractament suportarà la càrrega de demostrar el caràcter manifestament infundat o excessiu de la sol·licitud.

El consentiment

El consentiment de l'afectat per al tractament de les seues dades es modifica: cal que aquest siga més clar. D'altra banda, hi ha singularitats respecte al tractament de dades de menors que ens obliga a detenir-nos amb un poc més de detall. En la Llei 3/2918 hem de detenir-nos en els articles 6, 9 i 10, per al consentiment en general, i en particular en el 7 i en el 12.6, pel que fa a menors. En el RGPD hem d'anar als articles 4.11, 7 i 9 a què afegim el 8 per a parlar de menors.

Se'ns plantegen moltes preguntes. Per exemple: si tenim una relació contractual amb un client, s'ha de supeditar aquest contracte al consentiment del tractament? La resposta és NO. Si l'afectat no consent en el tractament per a finalitats no relacionades amb el contracte, això no ha de condicionar-ne l'execució. Això ens porta a un fet molt important:

El consentiment sempre s'ha de prestar a través d'una declaració o una clara acció afirmativa i quan siguen diverses les finalitats del tractament s'ha d'atorgar el consentiment per a cadascuna.

Per exemple, en un hospital privat no poden negar-nos l'atenció mèdica si no acceptem el consentiment perquè les nostres dades s'empren per a enviar-nos publicitat de la seua secció ortopèdica.

Per a les persones físiques ha de quedar totalment clar que s'estan recollint, utilitzant, consultant o tractant d'una altra manera dades personals que els concerneixen, així com la mesura en què les dites dades són o seran tractades.

El principi de transparència exigeix que tota informació i comunicació relativa al tractament de les dites dades siga fàcilment accessible i fàcil d'entendre, i que s'utilitze un llenguatge senzill i clar, i que evidencie tant els riscos, les normes, les salvaguardes i els drets relatius al tractament de dades personals, així com de la manera de fer valer-ne els drets en relació amb el tractament, com ara els fins específics del tractament de les dades personals han de ser explícits i legítims, i s'han de determinar en el moment de la recollida.

Apareix el terme *inequívoc*: això vol dir que es requereix que hi haja una declaració dels interessats o una acció positiva que indique l'acord de l'interessat.

És important subratllar que ha de ser verificable; el responsable ha de ser capaç de demostrar-ho.

Si es dona en una declaració escrita que també es referisca a uns altres assumptes, la sol·licitud de consentiment es presentarà de tal manera que es distingisca clarament dels altres assumptes, de manera intel·ligible i de fàcil accés i que utilitze un llenguatge clar i senzill, i done per fet que no serà vinculant cap part de la declaració que constituïsca infracció del Reglament.

L'interessat tindrà dret a retirar-ne el consentiment en qualsevol moment. Serà tan fàcil retirar el consentiment com donar-lo.

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

Un altre element d'interès per la seua sensibilitat és el registre de dades relatives a condemnes i infraccions penals, procediments i mesures de seguretat connexes. A més del que diuen els textos que manegem (llei i reglament), no oblidem la norma específica (Directiva (UE) 2016/680 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per les autoritats competents per a fins de prevenció, investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals, i a la lliure circulació de les dites dades i per la qual es deroga la Decisió Marc 2008/977/JAI del Consell).

En resum, aquest tractament tan particular s'ha de realitzar conforme a l'article 10 del Reglament i al que estableix el Sistema de registres administratius de suport a l'Administració de Justícia. Els tractaments de les dades de naturalesa penal distints als anteriors només seran possibles quan es porten a cap per advocats i procuradors i tinguen per objecte recollir la informació facilitada pels seus clients per a l'exercici de les seues funcions.

Quan el tractament es porta a cap amb el consentiment de l'interessat, el responsable del tractament ha de ser capaç de demostrar que aquell ha donat el seu consentiment a l'operació de tractament. En particular, en el context d'una declaració per escrit efectuada sobre un altre assumpte, hi ha d'haver garanties que l'interessat és conscient del fet que en 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 empre un llenguatge clar i senzill i que no continga clàusules abusives. Perquè s'emeta un informe sobre el consentiment, l'interessat ha de conèixer com a mínim la identitat del responsable del tractament i els fins del tractament als quals estan destinades les dades personals. El consentiment no s'ha de considerar lliurement prestat quan l'interessat no gaudisca de verdadera o lliure elecció o no puga denegar o retirar-ne 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 li concerneixen, com ara una declaració per escrit, inclusivament per mitjans electrònics, o una declaració verbal. Això podria incloure marcar una casella d'un lloc web a Internet, escollir 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 realitzades amb el mateix o els mateixos fins. Quan el tractament tinga diversos fins, s'ha de donar el consentiment per a cadascun. 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)[15].

Consentiment i menors

El primer dubte seria: Què és un menor? A partir de quines edats establim la frontera? La llei l'estableix en els 14 anys, amb les excepcions lògiques: els supòsits en què la llei exigeix l'assistència dels titulars de la pàtria potestat o tutela; a més, els titulares de la pàtria potestat poden exercir en nom i representació d'aquests menors els drets d'accés, rectificació, cancel·lació, oposició o uns altres que puguen correspondre'ls. Si mirem el RGPD, ens indica, en relació amb l'oferta directa a infants de serveis de la societat de la informació, que el tractament es considerarà lícit a partir dels 16 anys.

El tema dels menors és suficientment delicat perquè la llei els tracte amb detall, com veurem en aquest mateix text.

Davant de qualsevol dubte, la recomanació immediata és consultar les directrius sobre el consentiment en el sentit del Reglament (UE) 2016/679. (GRUPO DE TRABAJO DE PROTECCIÓN DE LAS PERSONAS (Grupo de trabajo del artículo 29), 2018)

[15] No cal que al·ludim a contraexemples. El consentiment és, probablement, en les dates que escrivim aquestes línies, el que pitjor sembla que han entès els professionals. Res d'estrany, tot i que sí resulta si més no cridaner que molts webs d'ajuntaments continuen sense actualitzar-ne els avisos legals i polítiques de privacitat i facen referència no ja a la LOPD, i ometen al·lusions al Reglament o a la Llei 3/2018, 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 "Leyes y ordenanzas nuevamente hechas por su Majestad para la gobernación de las Indias y buen tratamiento y conservación de los Indios".
Tanmateix, cal indicar un exemple no solament de desconeixement de la norma, sinó fins i tot de mala praxi claríssima: almenys en dos importants hospitals, gestionats per mans privades, he constatat que el consentiment es dona de manera implícita en signar el registre d'entrada al servei, amb les caselles premarcades i al·ludint que la no-acceptació d'alguna d'aquestes implica canvis en el servei i sobretot en el pagament ("En el caso de oponerse (…) será íntegramente de su cargo (…) el pago de los productos y/o servicios prestados").

El responsable del tractament davant de la inexactitud de les dades

La pregunta que ocupa el professional que treballa amb dades quan aquestes es demostren no exactes és, doncs, em poden imputar res per això? La resposta la porten els articles 4 i 5 de la Llei 3/2018 i els apartats d) i f) de l'article 5 del RGPD.

En resum, no seria imputable quan haja adoptat sense dilació les mesures raonables per a la supressió o rectificació i sempre que les dades:

- Les ha obtingudes el responsable directament de l'afectat o d'un registre públic o bé a través d'un mediador o intermediari; en aquest cas, aquest últim assumeix la responsabilitat.
- Les ha tractades el responsable després d'haver-les rebudes d'un altre responsable, en virtut de l'exercici de portabilitat.

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 distints estats hi han creat al llarg de les dècades les pròpies normes. Això, ho respecta el Reglament quan indica 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, preveu particularment que s'han d'incloure mesures específiques per a preservar la dignitat humana dels interessats, així com els seus interessos legítims i drets fonamentals, i posa l'accent especialment 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 al lloc de treball.

Què fem amb el correu electrònic dels treballadors? *A priori*, llegir un compte de correu aliè, tot i 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 se solen resumir a obtenir una ordre judicial, tret 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? A les empreses es fan revisions anuals per a saber si el treballador és apte o no per al treball que ha d'exercir, però aquests 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 sobre aquestes no es podrà realitzar cancel·lació, però sí una limitació de l'ús.

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

Actuacions del delegat de protecció de dades

Aquesta nova figura ens genera molts dubtes. El principal seria, doncs, quina organització ha de disposar d'un delegat? On encaixa i com arriba un a ser delegat de protecció de

dades (DPD)? La que pot ser més important és: Què ha de fer si es dona una reclamació? La Llei 3/18 ens ho conta en els articles 34, 35, 36 i 37, i el RGPD en els articles 37, 38 i 39.

Quines entitats han de tenir un DPD?

Entitat / camp	**Professionals**	Esport	Docència
	Els col·legis professionals i els seus consells generals.	Les federacions esportives quan tracten dades de menors d'edat.	Els centres docents que oferisquen ensenyaments en qualssevol dels nivells establits en la legislació reguladora del dret a l'educació, així com les universitats públiques i privades.
Entitat / camp	**Sanitat**		
	Els centres sanitaris legalment obligats al manteniment de les històries clíniques dels pacients. S'exceptuen els professionals de la salut que, tot i estar legalment obligats al manteniment de les històries clíniques dels pacients, exerceixen la seua activitat a títol individual.		
Entitat / camp	**Sector TIC**		
	Les entitats que exploten xarxes i presten serveis de comunicacions electròniques conforme al que disposa en la seua legislació específica, quan tracten	Els prestadors de serveis de la societat de la informació quan elaboren a gran escala perfils dels usuaris del servei.	Els operadores que desenvolupen l'activitat de joc a través de canals electrònics, informàtics, telemàtics i interactius, conforme a la normativa de

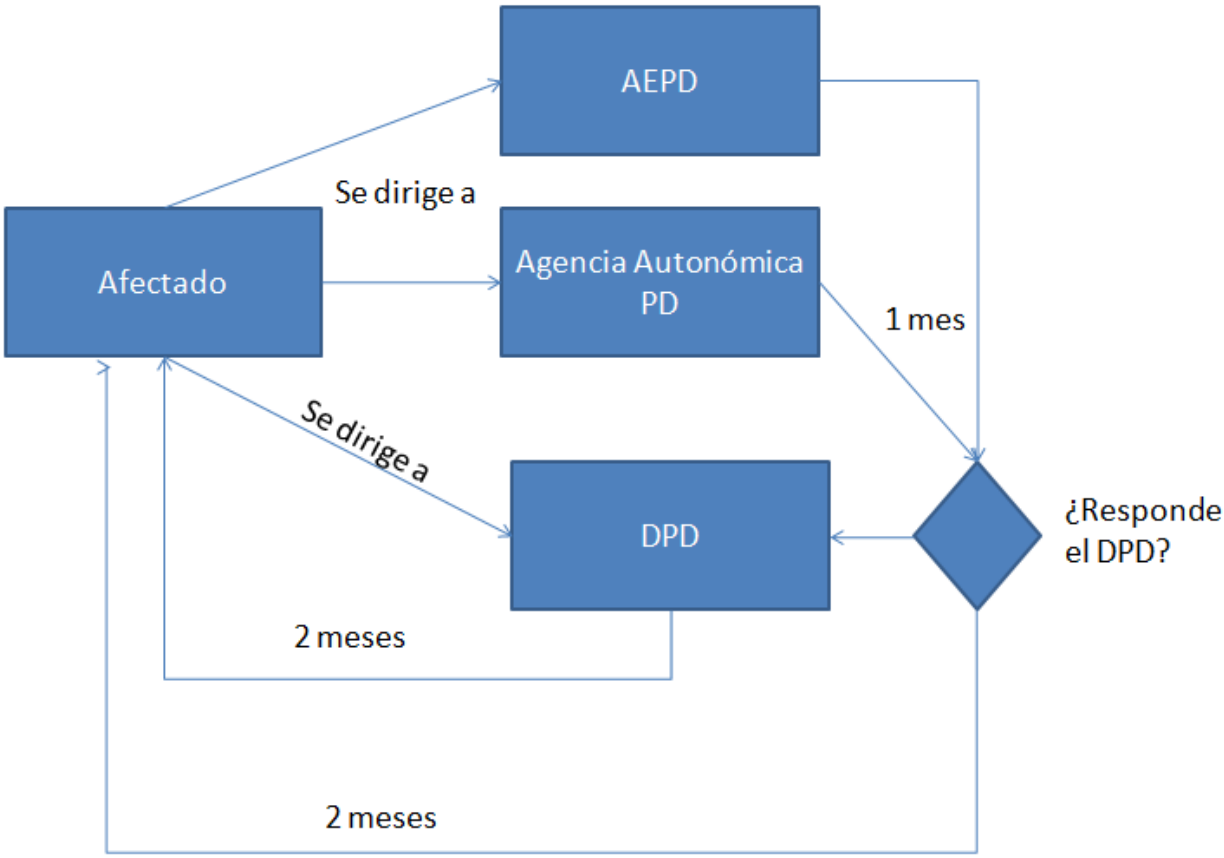
	habitualment i sistemàticament dades personals a gran escala.		regulació del joc.
Entitat / camp	**Economia, crèdit**		
	Les entitats incloses en l'article 1 de la Llei 10/2014, de 26 de juny, d'ordenació, supervisió i solvència d'entitats de crèdit.	Els establiments financers de crèdit.	Les empreses de serveis d'inversió, regulades per la legislació del Mercat de Valors.
	Les entitats que tinguen com un dels seus objectes l'emissió d'informes comercials que es puguen referir a persones físiques.		
Entitat / camp	**Seguretat, asseguradores**		
	Les entitats asseguradores i reasseguradores.	Les entitats responsables de fitxers comuns per a l'avaluació de la solvència patrimonial i crèdit o dels fitxers comuns per a la gestió i prevenció del frau, incloent-hi els responsables dels fitxers regulats per la legislació de prevenció del blanqueig de capitals i del finançament del terrorisme.	
Entitat / camp	**Grans empreses, publicitat**		
	Els distribuïdors i comercialitzadors d'energia elèctrica i els	Les entitats que desenvolupen activitats de publicitat	Les empreses de seguretat privada.

	distribuïdors i comercialitzadors de gas natural.	i prospecció comercial, incloent-hi les d'investigació comercial i de mercats, quan porten a cap tractaments basats en les preferències dels afectats o realitzen activitats que n'impliquen l'elaboració de perfils.	

Una pregunta típica és si un DPD ha d'estar certificat per alguna entitat. Tot i més: si pot no ser una persona *humana*, física, i al seu lloc ser una persona jurídica. No, no és obligatori certificar-se i no ha de ser per obligació una persona física. Però passar pels processos voluntaris de certificació (que consideren per a això la possessió d'una titulació universitària que acredite coneixements especialitzats en el dret i la pràctica en matèria de protecció de dades) és molt avantatjós.

Recordem que el DPD serà l'interlocutor amb l'Agencia i qui ha de documentar i actuar per vulneracions rellevants dels drets. Per això, no podrà ser acomiadat ni sancionat, tret que incórrega en dol o negligència greu, d'altra manera impediríem que actuara amb plena independència, i evitar qualsevol conflicte d'interessos. D'igual manera, no se li pot negar l'accés a les dades, sense que la confidencialitat puga invocar-se per a això.

Aquesta interlocució que indicàvem del DPD amb l'Agencia, i les seues actuacions davant d'una reclamació, podríem resumir-ho en la imatge següent:



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

Moltes vegades, el professional s'ha de fer càrrec d'unes dades de què no és el responsable del tractament, ni encarregat, ni tan sols membre de l'empresa on aquestes dades es gestionen. Pensem en una gestoria menuda que ha de fer els documents destinats a la seguretat social dels treballadors de les seues empreses clients. O pensem en una agència de viatges que intercanvia les dades dels seus clients amb la botiga de mobles que té davant, per a llançar-los publicitat. O reblem més el clau, 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 internacionals de dades

En aquest món cada vegada més menut, és estrany cenyir-se a les pròpies fronteres a l'hora de realitzar negocis. Moltes vegades es tracta de països que no solament estan al nostre entorn, sinó també en el nostre marc legal. D'altres, es tracta de tercers països amb una legislació en temes de privacitat inferior a la nostra. Cal seguir al peu de la lletra la norma, en concret els articles 40 a 43 de la Llei 3/2018 i els articles 44 a 50 del RGPD.

Veiem com l'existència de fluxos transfronterers de dades personals és necessari per al dia a dia de persones, negocis i institucions. Tanmateix, a mesura que s'incrementen aquests fluxos

proporcionalment creix la inquietud sobre la possible reducció o desaparició de la protecció de les nostres dades de caràcter personal.

Per això, és necessària l'avaluació del tercer país i considerar de quina manera s'hi respecta l'accés a la justícia i com les seues normes són o no homologables a la legislació europea. S'ha d'adoptar decisions que, considerant la legislació vigent en el tercer país, s'avalue si ofereix un nivell adequat de protecció equivalent essencialment a l'oferit respecte a les dades personals que són objecte de tractament, amb especial èmfasi en l'existència d'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 aleshores, pel seu compte, han de prendre mesures per a compensar la falta de protecció de dades en el tercer país. Aquestes mesures poden passar per normes corporatives vinculants o per clàusules tipus de protecció de dades (p. e. les facilitades per les autoritats de control). L'AEPD i les agències autonòmiques prepararan clàusules contractuals tipus per a la realització de transferències internacionals de pagament, sotmeses al dictamen del Comitè Econòmic Europeu.

Si no hi ha una decisió d'adequació de la Comissió, l'AEPD pot autoritzar prèviament transferències internacionals de dades, amb una durada màxima de sis mesos quan la transferència pretenga fonamentar-se en l'aportació de garanties adequades amb fonament en clàusules contractuals que no corresponen a les clàusules tipus, o quan la transferència es fonamente en disposicions incorporades a acords internacionals no normatius amb altres autoritats o organismes públics de tercers estats, que incorporen drets efectius i exigibles per als afectats, inclosos els memoràndums d'entesa i es porte a cap per algun dels responsables o encarregats relacionats en l'article 77.1

Amb aquestes garanties s'han d'assegurar els drets exigibles i la possibilitat d'accedir a accions legals efectives, i respectar 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 mediar en el consentiment explícit de l'interessat, i alhora la possibilitat de realitzar transferències quan així ho requereixen raons importants d'interès públic.

El deure d'informar sobre una transferència internacional a l'AEPD o autoritat autonòmica es dona sempre que es tracte d'una transferència sobre la base de la seua necessitat per a fins relacionats amb interessos legítims imperiosos perseguits pel responsable i no prevalguen els drets o interessos de l'interessat i es donen també els requisits següents: que no siga repetitiva, que afecte només un nombre limitat d'interessats i que el responsable haja avaluat totes les circumstancies concurrents. També s'informarà amb caràcter previ els afectats sobre la transferència i dels interessos legítims imperiosos perseguits, excepte si es realitza per les autoritats públiques en l'exercici dels seus poders públics.

Només es podran realitzar transferències internacionals de dades si el responsable o encarregat del tractament poden assegurar que el nivell de protecció de dades està garantit mitjançant:

- Decisió d'adequació presa per la Comissió de la UE.

- Garanties adequades de protecció de dades.

Sempre: contracte amb el receptor de dades, que hi especifique les garanties adequades.

Què ha de tenir en compte la Comissió en avaluar l'adequació del nivell de protecció? A tall 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 en el tercer país.

3. Els compromisos internacionals assumits pel tercer país 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 aquest tercer país o organització internacional ja no garanteix un nivell de protecció adequat, es derogarà, modificarà o suspendrà, en la mesura necessària i sense efecte retroactiu la decisió.

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

El responsable o l'encarregat del tractament només podran transmetre dades personals a un tercer país o organització internacional si haguera 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 adoptades per la Comissió

4. clàusules tipus de protecció de dades adoptades per una autoritat de control i aprovades per la Comissió

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

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

Si hi ha consentiment de l'autoritat de control, les garanties adequades podran ser aportades mitjançant:

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

Es poden preveu un seguit d'excepcions per a situacions específiques (Article 47), entre les quals destaquem les següents:

1. l'interessat haja donat explícitament el consentiment a la transferència proposada, després d'haver sigut informat sobre els possibles riscos;

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

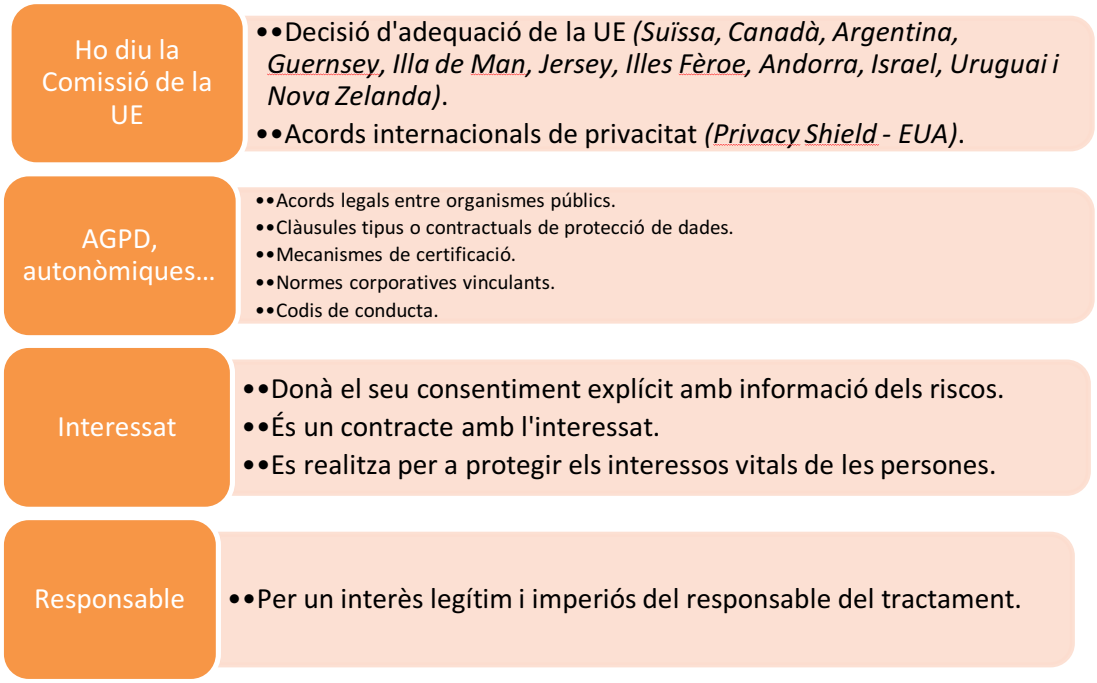
3. la transferència siga necessària per raons importants d'interès públic;

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

Posem-ne un exemple, que en si és tota una categoria: Estats Units. Els Estats Units òbviament no pertanyen a la Unió Europea, però els nostres fluxos comercials continus obliguen que s'arribe a una entesa en molts aspectes. En la privacitat, que és el nostre cas, es va fer el 26 de juliol de 2000 en signar un acord denominat *port segur* ("safeharbour") pel qual les empreses estatunidenques que complisquen uns requisits bàsics passen a formar part d'una llista que les permet la cessió de dades a aquestes. La informació respecte a això 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 superior que el que cadascun de nosaltres puga tenir. Per això posa salvaguardes legals, sabent que s'intentaran saltar, perquè l'alternativa, tallar qualsevol comunicació, és absolutament impensable.

Els propietaris de webs han de deixar-ne clara la finalitat: si és una pàgina web privada per a amics o coneguts o, si no hi ha dades personals, no cal fer-hi res. Però, i en el cas d'una associació? I si es tracta d'un club d'escalada? Aleshores estarem sotmesos a la regulació de la privacitat. Igual si som autònom, tindrem una sèrie de zones sensibles en el web, com ara el formulari de contacte, les dades dels clients que desitgen rebre les nostres novetats, l'enviament en si de correus electrònics, les galetes i fins i tot qui ha donat "m'agrada" en la nostra pàgina de Facebook.



Il·lustració 7. Licitud de les transferències. Adaptació de (Delgado Carravilla & Puyol Montero, 2018)

Què ha de fer el professional?

Respecte a l'interessat, cal:

- Informar sobre la intenció de realitzar transferències internacionals.
- Verificar l'existència o absència d'una decisió d'adequació.
- Obtenir garanties adequades i mitjans per a obtenir-ne còpia.

Respecte al registre d'activitats:

- Identificar les transferències internacionals.
- Documentar l'existència de garanties apropiades.

Articles de màxim interès per a entendre les transferències internacionals de dades.

Article 40 de la Llei 3/2018. Règim de les transferències internacionals de dades.

Article 41 de la Llei 3/2018. Supòsits d'adopció per l'Agencia Española de Protección de Datos.

Article 42 de la Llei 3/2018. Supòsits sotmesos a autorització prèvia de les autoritats de protecció de dades.

Article 43 de la Llei 3/2018. Supòsits sotmesos a informació prèvia a l'autoritat de protecció de dades competent.

RGPD. Article 44. Principi general de les transferències.

RGPD. Article 45. Transferències basades en una decisió d'adequació.

RGPD. Article 46. Transferències mitjançant garanties adequades.

RGPD. Article 47. Normes corporatives vinculants.

RGPD. Article 48. Transferències o comunicacions no autoritzades pel Dret de la Unió.

RGPD. Article 49. Excepcions per a situacions específiques.

RGPD. Article 50. Cooperació internacional en l'àmbit de la protecció de dades personals.

Cessió de dades i tractament per tercers

Si busquem aquestes figures en el Reglament, fent una cerca ràpida, veurem que no apareixen com a tals. Tanmateix, en un context com ara el nostre, i amb el precedent de la LOPD de 1999, i l'enorme treball desplegat respecte això des de fa temps enrere per l'Agencia Española de Protección de Datos, convé dedicar-hi un temps, ja que es tracta de dues situacions quotidianes que poden suggerir confusió atès que en ocasions no queden molt clares.

Cessió: Qualsevol revelació de dades realitzada a una persona distinta de l'interessat.

En la cessió de dades l'organització a què se cedeixen les dades farà en tractament per si mateixa, mentre que en el tractament per tercers, seran uns altres els que facen 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 adreça del cessionari. Se sol incloure una clàusula en què s'estableix que l'afectat accepta la cessió de les seues dades entre companyies del mateix grup i/o els seus agents comercials. No es considerarà comunicació de dades l'accés d'un tercer a la informació quan el dit accés siga necessari per a la prestació d'un servei a l'empresa. La realització de tractaments per compte de tercers ha d'estar regulada en un contracte que haurà de constar preferentment per escrit i, sinó, d'alguna manera que permeta acreditar-ne l'acord i contingut, i que establisca expressament que l'encarregat del tractament únicament tractarà les dades conforme a les instruccions del responsable del tractament, fet que implica que no les aplicarà o utilitzarà amb un fi distint al que consta en el dit contracte, ni les comunicarà, ni tan sols per a la seua conservació, a unes altres persones. A més, ha de constar en el contracte qualsevol 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 per a la seguretat social amb dades dels nostres treballadors o a una empresa de màrqueting perquè envie publicitat als nostres clients), és imprescindible regular aquest transvasament de dades a través d'un contracte en què el tercer que accedeix a la informació es comprometa a garantir el compliment de la llei en els mateixos termes que aquesta obliga el 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 dita comunicació tinguen el deure d'observar secret sobre les dades esmentades. I sembla obvi, pel que hem vist fins ara, que en enviar dades a tercers o

permetre-hi l'accés, aquestes només podran ser usades per al compliment de fins directament relacionats amb les funcions legítimes del cedent i del cessionari amb el consentiment previ 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 realitza 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 seran recollides les dades de caràcter personal així com la forma d'exercir-hi els drets.

Singularitats a considerar pel professional

En aquesta mena de calaix de sastre tractarem alguns temes amb difícil classificació en les anteriors categories, però que tenen gran interès per al professional.

Les galetes

No solament es necessita recollir el consentiment per al tractament de dades personals, sinó que també hi ha casos, com ara la instal·lació de les galetes, on és obligatori.

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

En tot cas, el responsable ha de recordar que quan la instal·lació i/o utilització d'una galeta implique el tractament de dades personals, els responsables d'aquest tractament s'hauran d'assegurar del compliment de les exigències addicionals establides per 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.

Galetes exceptuades: les que tenen per finalitat:

- Galetes d'«entrada de l'usuari».
- Galetes d'autenticació o identificació d'usuari (únicament de sessió).
- Galetes de seguretat de l'usuari.
- Galetes de sessió de reproductor multimèdia.
- Galetes de sessió per a equilibrar la càrrega.
- Galetes de personalització de la interfície d'usuari.
- Galetes de complement (connector o *plug-in*) per a intercanviar continguts socials.

La informació sobre les galetes facilitada en el moment de sol·licitar el consentiment ha de ser suficientment completa per a permetre als usuaris entendre la finalitat perquè s'instal·laren i conèixer els usos que s'hi donaran.

Si és necessari obtenir el consentiment per a la instal·lació de les galetes per usuaris ja registrats caldrà que informar-los de manera verificable sobre els canvis realitzats en relació amb el tractament de les galetes.

Contractació de serveis d'informàtica en núvol o "Cloud Computing"

És important identificar quins proveïdors del núvol estan localitzats dins de l'Espai Econòmic Europeu. Localització no solament de la seu del proveïdor, sinó dels seus recursos físics. La contractació de serveis d'informàtica en núvol es realitzarà 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-ne els termes.

El responsable ha de decidir per a quines dades personals contractarà serveis d'informàtica en núvol i quins prefereix mantenir en els seus sistemes d'informació. Aquesta decisió és important perquè delimitarà les finalitats per a les quals el proveïdor del núvol 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 d'informàtica en núvol.

Perquè el responsable es puga assegurar 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 què és responsable. El responsable, com a client, ha de ser informat diligentment pel proveïdor del núvol sobre les incidències de seguretat que afecten les dades de què el mateix 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 es puguen produir.

Normes d'alt interès a considerar:

- Llei de Contractes del Sector Públic. (RD Legislatiu 3/2011, de 14 de novembre).

- Llei 11/2007 d'Accés Electrònic dels Ciutadans als Serveis Públics i RD 1671/2009 que desplega 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).

Sistemes d'informació de denúncies internes

Desplegat en l'article 24 de la Llei 3/2018, se'ns explica com cal actuar amb la informació de possibles incompliments legals, ètics o de normativa interna, que puga donar pas a sancions o a denúncies davant de la justícia.

Qui pot accedir a aquestes dades? Aquests sistemes que poden servir per a posar en coneixement d'una entitat de dret privat, fins i tot anònimament, la comissió d'infraccions tindran un accés limitat per la sensibilitat de la informació que conté. Aquest accés serà només per als que desenvolupen les funcions de control intern i de compliment, els encarregats del tractament designats per a això i als que resulte necessari per a l'adopció de mesures disciplinàries o per a la tramitació de procediments judicials. Només en el cas que es puguen

adoptar mesures disciplinàries contra un treballador es permetrà al personal amb funcions de gestió i control de recursos humans.

S'han de tenir en compte un seguit de consideracions, com ara que tant empleats com tercers hauran de ser informats sobre l'existència d'aquests sistemes d'informació, la necessitat d'adoptar mesures per a preservar la identitat i garantir la confidencialitat de les dades, especialment del denunciant. Les dades s'hauran de conservar únicament durant el temps imprescindible per a decidir sobre la procedència d'iniciar una investigació.

Sobre la videovigilància

La norma en parla de dues maneres molt concretes: sobre els mateixos treballadors (art. 89 3/2018) i en general (clients...), en l'art. 22. Es deixa clar que només es pot realitzar en la via pública quan és imprescindible per a preservar la seguretat, però amb una sèrie de condicionants.

- Es pot captar una extensió superior quan calga per a garantir la seguretat de béns o instal·lacions estratègics o d'infraestructures vinculades al transport, sempre que no supose la captació d'imatges de l'interior d'un domicili privat.
- Excepte quan s'hagen de conservar per a acreditar la comissió d'un delicte, seran suprimides en el termini màxim d'un mes des de la captació. Si es dona el cas, les imatges hauran de ser posades a disposició de l'autoritat competent en un termini màxim de setanta-dues hores des que es tinguera coneixement de l'existència de l'enregistrament.
- El deure d'informació s'entendrà complit mitjançant la col·locació d'un dispositiu informatiu en un lloc suficientment visible que identifique, almenys, l'existència del tractament, la identitat del responsable i la possibilitat d'exercir els drets previstos en els articles 15 a 22 del Reglament (UE) 2016/679.
- Queda exclòs el tractament per una persona física d'imatges que solament capten l'interior del propi domicili (sempre que no ho faça una entitat de seguretat privada que haguera sigut contractada per a la vigilància d'un domicili i tinguera accés a les imatges).

Exclusió publicitària

Les velles i conegudes llistes Robinson cobren actualitat amb l'art. 23 de la Llei 3/2018. En parlàrem en analitzar la limitació del tractament.

En tractar-se d'una llista per a no estar-ne en cap, cal preguntar-se si és lícit aquest tractament. I si es poden crear sistemes d'informació en què només s'inclouran les dades imprescindibles per a identificar els afectats, de manera que es puga eliminar la recepció de comunicacions comercials.

Se n'ha de comunicar a l'AEPD o agències autonòmiques la creació, caràcter, mode d'incorporar-se al sistema i com fer-ne valer les preferències. L'autoritat de control farà pública a la seua seu electrònica una relació dels sistemes i el posarà en coneixement de les restants autoritats de control per a la publicació per totes aquestes. Quan un afectat manifeste el desig que les seues dades no siguen tractades, aquest haurà d'informar-li dels sistemes d'exclusió publicitària existents. Els que pretenguen realitzar comunicacions de màrqueting directe, prèviament hauran de consultar els sistemes d'exclusió publicitària que puguen afectar-ne l'actuació.

No caldrà realitzar la consulta quan l'afectat n'haguera prestat el consentiment per a rebre la comunicació a qui pretenga realitzar-la.

Informació creditícia

Els deutes, la seua reclamació..., sempre han sigut un dels punts més calents de la normativa sobre protecció de dades. L'article 20 de la Llei 3/2018 versa sobre aquest espinós tema. Quan es pot fer un tractament de dades personals relatiu a l'incompliment de les obligacions de pagament? S'han de donar les condicions següents:

a) Que les dades hagen sigut facilitades pel creditor o per qui actue pel seu compte o interès.

b) Que les dades es referisquen a deutes certs, vençuts i exigibles, l'existència o quantia dels quals no haguera sigut objecte de reclamació administrativa o judicial pel deutor o mitjançant un procediment alternatiu de resolució de disputes vinculant entre les parts.

c) Que el creditor haja informat l'afectat en el contracte o en el moment de requerir el pagament sobre la possibilitat d'inclusió en els dits sistemes, amb indicació dels que participa. L'entitat que mantinga el sistema d'informació creditícia amb dades relatives a l'incompliment d'obligacions dineràries, financeres o de crèdit haurà de notificar l'afectat sobre la inclusió d'aquestes dades i li informarà sobre la possibilitat d'exercir els drets establits.

d) Que les dades únicament es mantinguen en el sistema mentre persistisca l'incompliment, amb el límit màxim de cinc anys des de la data de venciment de l'obligació dinerària, financera o de crèdit.

i) Que les dades referides a un deutor determinat solament puguen ser consultades quan qui consulte el sistema mantinguera una relació contractual amb l'afectat que implique l'abonament d'una quantia pecuniària o aquest l'haguera sol·licitat la celebració d'un contracte que supose finançament, pagament ajornat o facturació periòdica, com succeeix, entre altres supòsits, en els previstos en la legislació de contractes de crèdit al consum i de contractes de crèdit immobiliari.

f) Que, en el cas que es denegara la sol·licitud de formalitzar el contracte, o aquest no arribara a signar-se, com a conseqüència de la consulta efectuada, qui haja consultat el sistema informe l'afectat sobre el resultat de la dita consulta.

Empresaris autònoms, professió liberal

El teixit empresarial que ens envolta està en gran mesura compost de petites empreses; més i tot, microempreses i fins i tot professionals i treballadors que amb una llicència d'autònom es constitueixen en empresa. Aquestes diminutes empreses no disposen, òbviament, d'informàtics en plantilla, però sí recorren a l'assessorament extern. Moltes vegades ens preguntaran, doncs, què passa amb les dades dels meus clients? Una visió d'això ha de passar per l'article 19 de la Llei 3/2018 i la definició de tractament lícit que se'ns dona en el 6.1.f) del RGPD.

Què passa amb les dades que conserven els professionals liberals? *A priori* és lícit el tractament de dades, ja que s'entén que aquest és necessari per a la satisfacció d'interessos legítims perseguits pel responsable del tractament (el petit empresari) o per un tercer (un

gestor), sempre que sobre els dits interessos no prevalguen els interessos o els drets i llibertats fonamentals de l'interessat que requerisquen la protecció de dades personals. A la recíproca, la mateixa presumpció serveix per al tractament de les dades relatives als empresaris individuals i als professionals liberals, quan s'hi referisquen únicament en la dita condició i no es tracten per a establir-hi una relació com a persones físiques.

Òbviament, parlem tan sols de les dades necessàries per a la seua localització professional.

Tractaments de dades amb peculiaritats

En aquest apartat anirem un pas més enllà. Hem vist com hi ha un seguit de dades que la legislació protegeix amb zel. Veurem com interpreta això el Reglament i la Llei 3/2018, alhora que veurem què succeeix amb elements peculiars, com ara les dades dels finats o les dels infants. Algunes, com ara les dades relatives a condemnes i infraccions penals (Article 10) ja s'han vist en altres parts d'aquest tema.

Categories especials de dades personals

Hi ha un seguit 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 adreçades 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. És convenient visitar l'article 9 del RGPD en aquest punt.

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

1. Si l'interessat donà el consentiment explícit per al tractament de les dites dades personals amb un o més dels fins especificats (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 és efectuat, en l'àmbit de les seues activitats, per 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 fins 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 fins d'arxiu en interès públic, fins d'investigació científica o històrica o fins estadístics.

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

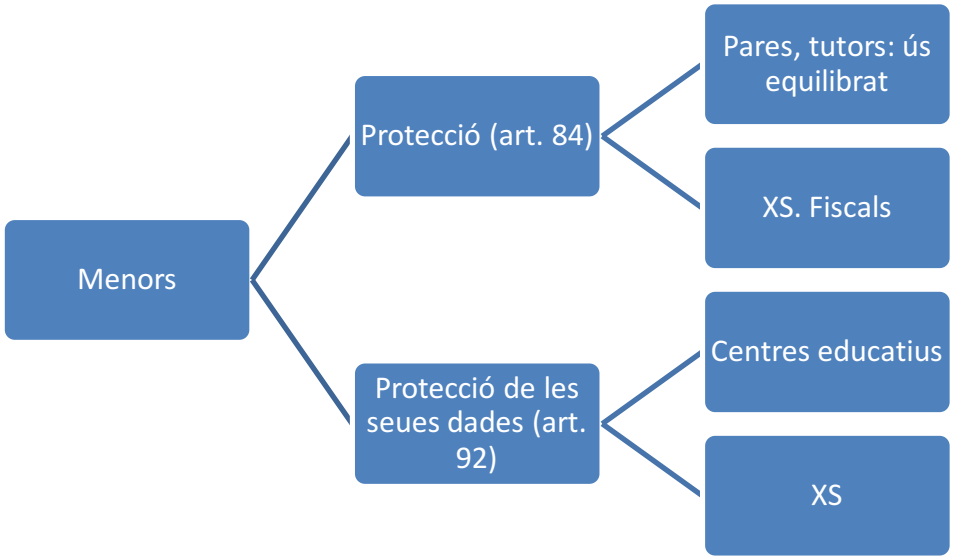
El tractament de categories especials de dades personals, sense el consentiment de l'interessat, pot ser necessari per raons d'interès públic en l'àmbit de la salut pública. Així, s*alut pública* s'ha d'interpretar com tots els elements relacionats amb la salut, concretament l'estat de salut, amb inclusió 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 disposició d'assistència sanitària i l'accés universal a aquesta, 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 a que tercers, com ara empresaris, companyies d'assegurances o entitats bancàries, tracten les dades personals amb altres fins. (Considerant 54)

Infants

Els infants mereixen una protecció específica, ja que són menys conscients dels riscos, conseqüències, garanties i drets concernents al tractament de dades personals. Això és de particular importància quan es tracta de l'ús de les seues dades amb fins de màrqueting o elaboració de perfils de personalitat o d'usuari. (Considerant 38) (Article 8 RGPD)

Si es fan ofertes directes a infants, el tractament de les dades personals d'un xiquet es considerarà lícit quan tinga com a mínim 16 anys. Si el xiquet és menor, únicament serà lícit si el consentiment el donà o autoritzà el titular de la pàtria potestat o tutela sobre l'infant. El màxim de 16 anys podrà ser rebaixat pels estats membres, però de manera que no siga mai inferior a 13 anys.

Considerem que a penes hi ha serveis que permeten saber l'edat d'algú. Això és així per la complexitat de 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 en compartir ordinador amb ells. Per a més informació sobre infants, xarxes socials i privacitat, es recomana la consulta de (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). També de les Pautes de protecció de dades per als centres educatius, publicades per l'Agència Catalana de Protecció de Dades (Agencia Catalana de Protección de Datos, 2018).



Il·lustració 8. Títol X i menors, elaboració pròpia

Condemnes i infraccions penals

Només es pot efectuar sota la supervisió de les autoritats públiques, amb garanties adequades per als drets i llibertats dels interessats. (Article 10 RGPD)

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 de 2016, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per les autoritats competents per a fins de prevenció, investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals, i a la lliure circulació de les dites dades i per la qual es deroga la Decisió Marc 2008/977/JAI del Consell (Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, 2016)

Finats

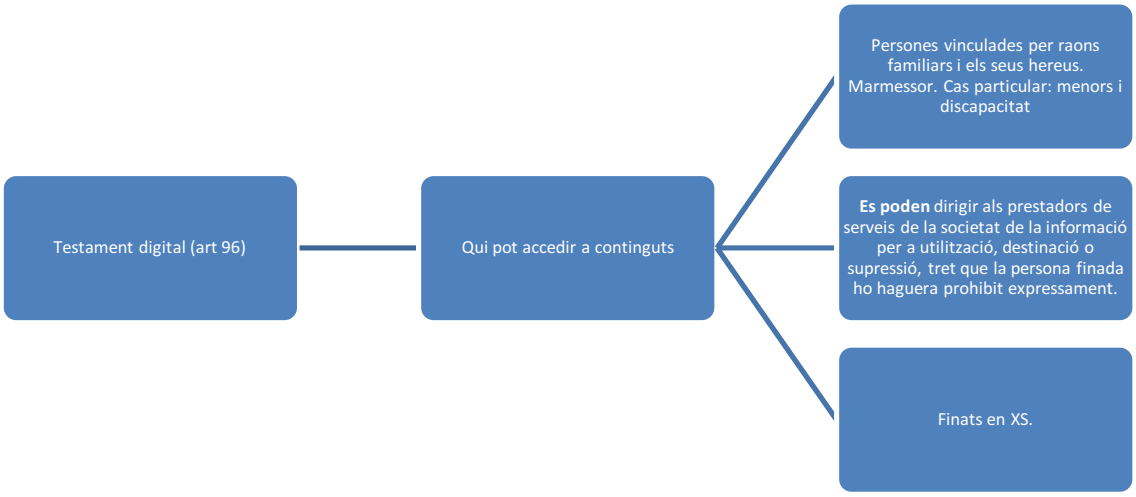
El Reglament no s'aplica a la protecció de dades personals de persones mortes, tot i que els estats membres hi poden establir normes relatives. S'ha de considerar l'autorització per a establir el tractament ulterior de dades personals amb fins d'arxiu i amb fins d'investigació històrica, incloent-hi la investigació per a fins genealògics i per causes greus, com per exemple, genocidi. (Considerants 27, 158 i 160)

Segons la Llei 3/2018:

Es permet que les persones vinculades al finat per raons familiars o de fet o els seus hereus puguen sol·licitar-hi l'accés, així com la rectificació o supressió, si és el cas amb subjecció a les instruccions del finat.

No podran accedir a les dades del causant, ni sol·licitar-ne la rectificació o supressió, quan la persona morta ho haguera prohibit expressament o així ho establisca una llei.

En cas de mort de menors i persones amb discapacitat, aquestes facultats es podran exercir també pels seus representants legals o, en el marc de les seues competències, pel Ministeri Fiscal.



Il·lustració 9. Títol X i testament digital. Elaboració pròpia

Tractament amb fins d'arxiu en interès públic, fins d'investigació científica o històrica o fins estadístics

S'ha 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 ara la pseudonimització. Quan l'exercici dels drets derivats del tractament de dades personals amb fins d'investigació científica o històrica o estadístiques impossibiliten o obstaculitzen greument l'obtenció dels fins científics, es podran establir excepcions. (Article 89)

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

Per fins estadístics s'entén qualsevol operació de recollida i tractament de dades personals necessàries per a enquestes estadístiques o per a la producció de resultats estadístics. Aquests

resultats estadístics, a més, es poden utilitzar amb diferents fins, inclosos fins d'investigació científica. El fi estadístic implica que el resultat del tractament amb fins estadístics 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

Ja sabem de dades que impliquen una intimitat molt especial. D'entre aquestes, les creences religioses i les idees polítiques figuren entre les destacades. Respecte a això, les esglésies, associacions o comunitats religioses estan subjectes a la supervisió d'una autoritat de control. Òbviament no se'ls pot impedir tot tractament, ja que aleshores la seua gestió del dia a dia seria impossible. (Article 91)

Tractament i accés públic de documents oficials

De nou ens trobem amb una altra qüestió de drets que se superposen. En aquest cas a privacitat enfrontem transparència. Com fer públic què és privat? De quina manera una dada personal pot ser transparent? Respecte a això, 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 podran ser comunicats per la dita 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. (Article 86)

Es té en compte el principi d'accés del públic als documents oficials, que és un fet 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. S'ha de parar esment particular als documents a què no es puga accedir o l'accés als quals està 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 haja quedat 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 a aquest respecte la consulta de la 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 (DO L 345 de 31.12.2003, p. 90). (PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA, 2003)

Altres dades especialment protegides

Hi ha dades que, per la seua naturalesa, són particularment sensibles en relació amb els drets i les llibertats fonamentals, ja que el context del seu tractament podria comportar importants riscos: entre els quals apareixen les dades de caràcter personal que revelen l'origen racial o ètnic. (Considerants 51 i 51!)

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 permet la identificació o l'autenticació unívoques d'una persona física.

Aquestes dades personals no han de ser tractades, tret que se'n permeta el tractament en situacions específiques. S'han d'establir de forma explícita excepcions, entre altres quan l'interessat en done el consentiment explícit o tractant-se de necessitats específiques.

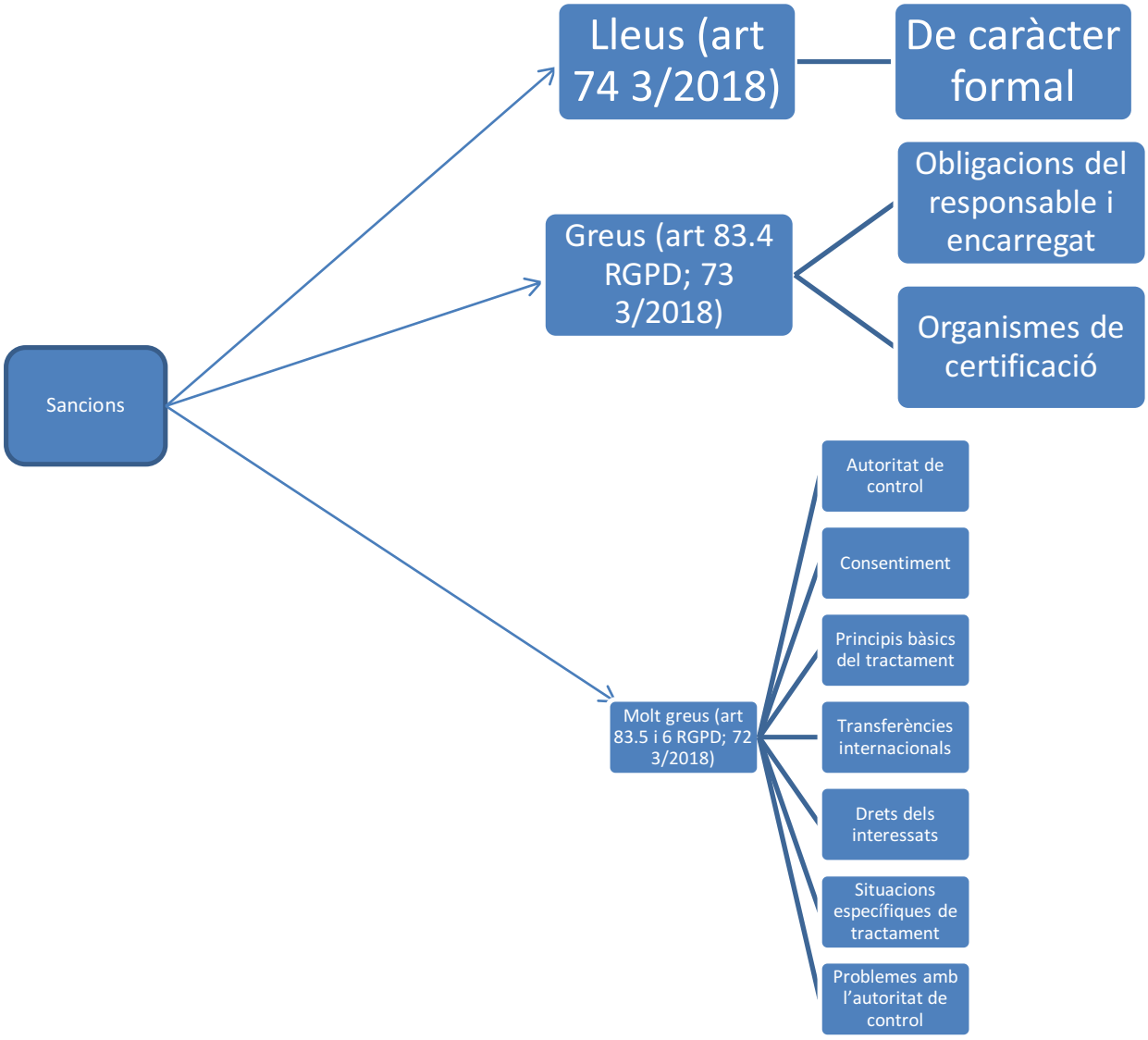
Altres excepcions: sempre que es donen les garanties apropiades, en interès públic, en particular el tractament de dades personals en l'àmbit de la legislació laboral, la legislació sobre protecció social, incloses les pensions i amb fins de seguretat, supervisió i alerta sanitària, la prevenció o control 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.

Règim sancionador

Una de les zones més denses en la norma (títol IX en la Llei 3/2018, articles 10 a 78 i articles 83 i 84 del RGPD) és el de les sancions. La primera pregunta seria a qui es pot sancionar? A això respon l'article 70, que refereix a responsables i encarregats dels tractaments, i als seus representants quan es tracta d'entitats no establides en el territori de la Unió Europea, i les entitats de certificació i les acreditades de supervisió dels codis de conducta. Deixa fora d'aquest conjunt el DPD.

Hi ha una llarga relació en la norma que ens permet classificar infraccions i sancions. A tall de resum, indiquem que ambdues es classifiquen en lleus, greus i molt greus.

Tractem de fer un esquema de les infraccions i sancions.



Il·lustració 10. Sancions. Elaboració pròpia

Al marge de la possibilitat d'exercir qualsevol acció judicial o recurs administratiu, l'interessat podrà presentar una reclamació davant d'una autoritat de control, la qual informarà 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 aquesta.

En el cas d'una tutela judicial contra un responsable o encarregat del tractament, aquesta s'exerceix davant dels tribunals de l'estat membre en què el responsable o encarregat tinga un establiment. Però també es podran exercitar davant dels tribunals de l'estat membre en què l'interessat tinga la seua residència habitual, tret 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 tindrà dret a rebre del responsable o l'encarregat del tractament una indemnització.

Qui respon dels danys? Qualsevol responsable que participe en l'operació de tractament respondrà dels danys i perjudicis causats en cas que la dita operació no complisca el que disposa el present Reglament. Un encarregat únicament respondrà dels danys i perjudicis causats pel tractament quan no haja complit amb 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 haja causat els danys, estaran exempts de responsabilitat. Si el dany és ocasionat per diversos encarregats o responsables, cadascun serà responsabilitzat, a fi de garantir la indemnització. En aquests casos, si un responsable o encarregat del tractament paga una indemnització total pel perjudici ocasionat, tindrà dret a reclamar als altres la part de la indemnització corresponent.

Qualsevol infracció d'aquest ha de ser castigada amb sancions, incloses multes administratives, amb caràcter addicional a mesures adequades imposades per l'autoritat de control.

Si es tracta d'una infracció lleu, o si la multa que probablement s'impose constitueix una càrrega desproporcionada per a una persona física, en lloc de sanció mitjançant multa es pot imposar una advertència. 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. Tanmateix, la imposició de sancions penals per infraccions de les dites normes nacionals i de sancions administratives no ha d'implicar la vulneració del principi *ne bis in idem* ("No dues vegades pel mateix fet").

Les autoritats de control garantiran que les multes administratives siguen en cada cas efectives, proporcionades i dissuasives. Per a determinar-ne la quantia es tindrà en compte (entre d'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 preses pel 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 a fi 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 tingué coneixement (el responsable o l'encarregat notificaren la infracció?);
8. L'adhesió a codis de conducta.

Es produeix un enduriment del règim sancionador, ja que les sancions poden arribar fins als 20 milions d'euros o el 4% del volum de negoci total anual global de l'exercici financer anterior, la quantitat més alta. Per a la quantia de les multes administratives, s'aconsella consultar el Reglament i la legislació nacional.

Drets digitals. Títol X

Un dels elements distintius de la Llei 3/2018 és el títol X, on es presenten una sèrie de drets digitals. La llei expressa el desig del legislador d'assolir-ne en una futura reforma de la Constitució una actualització a l'era digital i, amb això, elevar a rang constitucional una nova generació de drets digitals.

Atès que la reforma és un fet en aparença llunyà, aprofitant el gran tren de la llei de Protecció de Dades, se suma un vagó específic que busca abordar el reconeixement d'un sistema de garantia dels drets digitals que, com la resta de la llei, naix del mandat de l'apartat quart de l'article 18 de la Constitució espanyola. Cal especificar que en alguns casos ja han sigut perfilats per la jurisprudència ordinària, constitucional i europea.

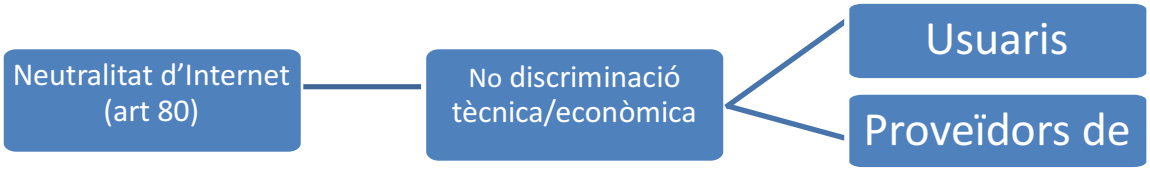
Vegem-los.

Il·lustració 11. Drets digitals. Elaboració pròpia.

1. Dret a la neutralitat d'Internet

Això va lligat a l'anomenada Internet de dues velocitats. Posem-ne un exemple: Si Toni des de sa casa vol fer un vídeo i penjar-lo a Vimeo sobre com fer macramé a les fosques, un deport amb pocs seguidors i no patrocinat per ningú, i son pare, el Sr. Antoni, gaudirà del partit de la Final de la Copa entre el Pedregar FC i el Pedreguer CF, pot veure com la seua connexió va més lenta que la de son pare, perquè una operadora ha establit un canal de pagament més ràpid per a visualitzar el matx de futbol.

El que implica la neutralitat de la xarxa és que tots els paquets de dades que viatgen per Internet s'han de tractar de la mateixa manera, independentment del contingut. "Els proveïdors de serveis d'Internet proporcionaran una oferta transparent de serveis sense discriminació per motius tècnics o econòmics".

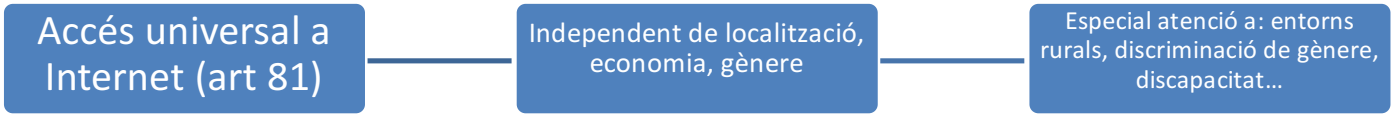


Il·lustració 12. Neutralitat d'internet. Elaboració pròpia.

2. Dret d'accés universal a Internet

En virtut d'aquesta llei, l'estat ha de garantir "un accés universal, assequible, de qualitat i no discriminatori per a tota la població", de manera que "Tots tenen dret a accedir a Internet independentment de la seua condició personal, social, econòmica o geogràfica", i que preveu

"accions dirigides a la formació i l'accés a les persones majors" i atenció a la població rural i persones que tinguen necessitats especials.



Il·lustració 13. Dret d'accés universal.

3. Dret a la seguretat digital

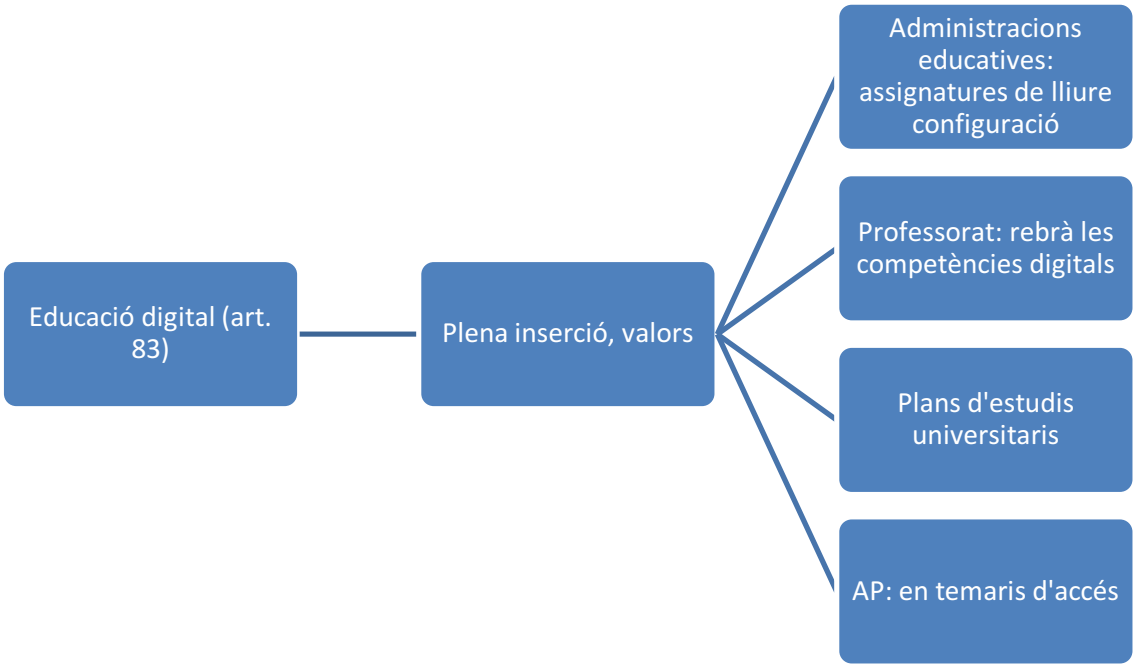
És una passa nova a un clàssic: el dret a la privacitat de les comunicacions. Se subratlla que "els proveïdors de serveis d'Internet informaran els usuaris sobre els seus drets".

Il·lustració 14. Seguretat digital. Elaboració pròpia.

4. Dret a l'educació digital

El model actual d'educació se subjecta sobre competències logicomatemàtica, social, lingüística…, a què s'afegeix la *competència digital*, que ja era des de 2014 en educació primària una "competència bàsica". Les comunitats autònomes han de considerar aquesta inclusió en tots els plans educatius, en què aquest ús ha de ser "segur i respectuós amb la dignitat humana, els valors constitucionals, els drets fonamentals i, particularment, amb el respecte i la garantia de la intimitat personal i familiar i la protecció de dades personals".

També afecta les universitats, on els alumnes de qualsevol titulació han de saber manejar els mitjans digitals, i seran incloses proves específiques sobre això en les oposicions.



Il·lustració 15. Educació digital. Elaboració pròpia.

5. Protecció dels menors a Internet

Es carrega en les obligacions de pares i tutors que "els menors d'edat facen un ús equilibrat i responsable dels dispositius digitals" per a "garantir el desenvolupament adequat de la seua personalitat i preservar-ne la dignitat i drets fonamentals". Si es donara una "intromissió il·legítima en els seus drets fonamentals" (recordem recents casos d'abusos usant xarxes socials), serien perseguides per defecte per la Fiscalia.

Qualsevol que desenvolupe activitats amb menors d'edat ha de tenir el consentiment del menor o dels seus representants legals.

6. Dret de rectificació a Internet

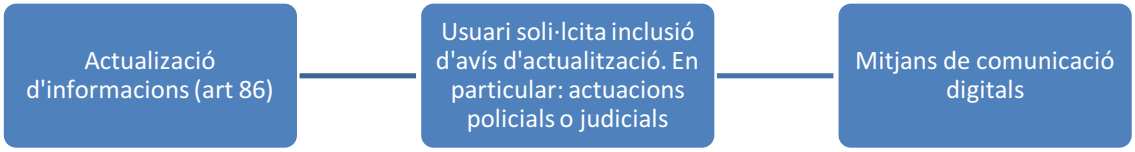
Ací ens trobem amb un dret ja recollit en una llei (de 1984 i, per tant, gens adaptada a l'entorn digital) que s'ha tornat a redactar per a adaptar-lo a la xarxa, de manera que si s'emeten dades inexactes o falses en mitjans de comunicació o, i això és nou, en comentaris de xarxes socials, es podrà exercir el dret de rectificació per vulneració de l'honor o la intimitat.

Il·lustració 16. Rectificació. Elaboració pròpia.

7. Dret a l'actualització d'informacions en mitjans de comunicació digitals

Si una noticia publicada ha deixat de reflectir la situació actual d'una persona "que li causa un perjudici" (per exemple amb una sentència que invalida d'altra anterior o amb el pagament

d'una quantitat endeutada) es pot "sol·licitar motivadament dels mitjans de comunicació digitals la inclusió d'un avís d'actualització suficientment visible junt amb les notícies que li concernisquen ".



Il·lustració 17. Actualització d'informacions. Elaboració pròpia.

8. Relatius als treballadors: dret a la intimitat i ús de dispositius digitals en l'àmbit laboral, dret a la desconnexió digital en l'àmbit laboral, dret a la intimitat enfront de l'ús de dispositius de videovigilància i d'enregistrament de sons al lloc de treball, dret a la intimitat enfront de la utilització de sistemes de geolocalització en l'àmbit laboral i drets digitals en la negociació col·lectiva.

Estem davant d'una sèrie de drets que tenen un nexe comú: el treballador.

8.1. Dret a la intimitat i ús de dispositius digitals en l'àmbit laboral.

En aquest cas es tracta de la privacitat dels treballadors, públics i privats, pel que fa a l'ús dels dispositius electrònics necessaris per al treball (telèfons, portàtils, tauletes…) que els subministre el seu ocupador. L'ocupador només podrà accedir-hi per a "controlar el compliment de les obligacions laborals o estatutàries i de garantir la integritat dels dits dispositius". Per a això "hauran d'establir criteris d'utilització dels dispositius digitals".

8.2 Dret a la desconnexió digital en l'àmbit laboral.

No es podran emprar eines digitals (enviar un WhatsApp, per exemple) per a contactar amb els seus treballadors fora de l'horari laboral o durant els seus períodes de descans.

8.3 Dret a la intimitat enfront de l'ús de dispositius de videovigilància i d'enregistrament de sons al lloc de treball.

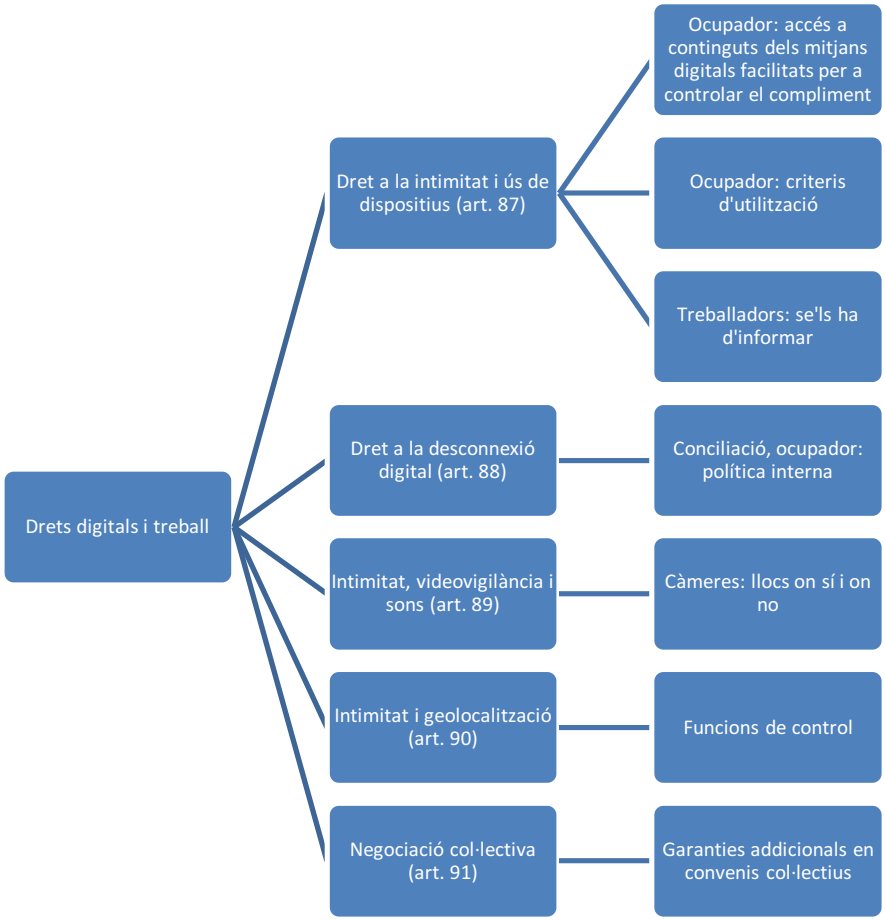
Es podran instal·lar càmeres per al control dels treballadors, però només es podran instal·lar micròfons quan "resulten rellevants els riscos per a la seguretat de les instal·lacions, béns i persones derivats de l'activitat que es desenvolupe al centre de treball" i en cap cas en vestidors, lavabos, menjadors o llocs destinats a l'esbarjo dels treballadors.

8.4 Dret a la intimitat enfront de la utilització de sistemes de geolocalització en l'àmbit laboral.

Es podran usar sistemes de geolocalització per a comprovar la ubicació dels treballadors, sempre que s'informe a ells i als seus representants "sobre l'existència i característiques d'aquests dispositius", i sobre els seus drets respecte d'això.

8.5 Drets digitals en la negociació col·lectiva.

Els convenis col·lectius podran establir "garanties addicionals dels drets i llibertats relacionats amb el tractament de les dades personals dels treballadors i la salvaguarda de drets digitals en l'àmbit laboral".

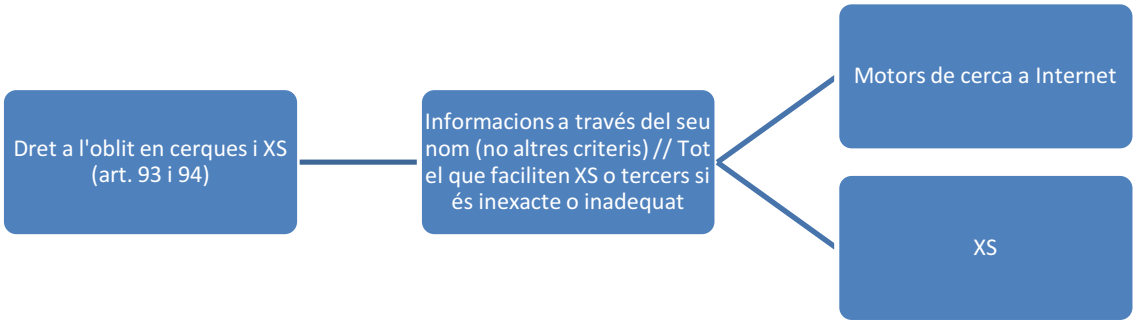


Il·lustració 18. Drets digitals i treball. Elaboració pròpia.

9. Dret a l'oblit en cerques d'Internet

El dret a l'oblit apareix expressament en la Llei 3/2018 i en el RGPD. Tanmateix, se'n reconeix la importància incloent-la entre els anomenats "drets digitals".

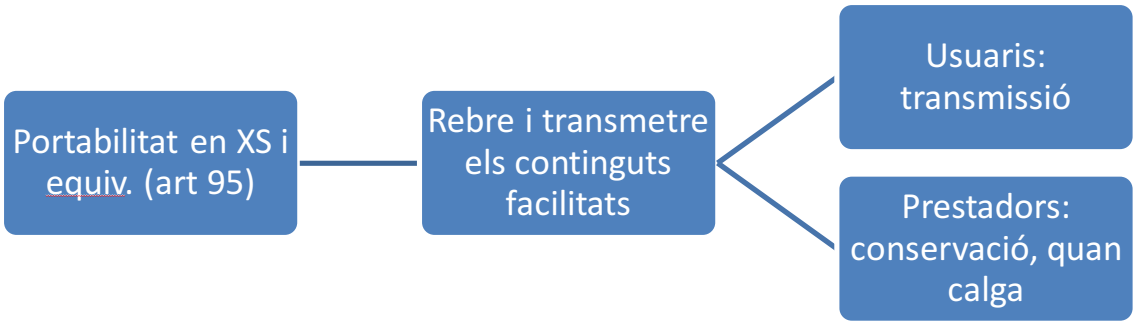
D'una banda, es tracta d'impedir que els cercadors associen informació antiga d'una persona, i permetre exercir-lo quan les dades que apareguen siguen "inadequades, inexactes, no pertinents, no actualitzades o excessives o hagueren esdevinguts com a tals pel transcurs del temps, tenint en compte els fins per als quals es recolliren o tractaren, el temps transcorregut i la naturalesa i interès públic de la informació". A més d'això, que sembla que és el que s'assumeix clàssicament com a dret a l'oblit, apareix una variant en xarxes socials i equivalents: "tota persona té dret que se suprimisquen les dades personals que li concerneixen i que hagen sigut facilitades per tercers per a la publicació pels serveis de xarxes socials" quan aquestes siguen "inadequades, inexactes, no pertinents, no actualitzades o excessives". Si, a més, la pujada d'aquestes dades a les xarxes socials s'haguera produït durant la minoria d'edat de l'afectat, aquesta retirada s'haurà de produir "sense dilació".



Il·lustració 19. Dret a l'oblit. Elaboració pròpia.

10. Dret de portabilitat en serveis de xarxes socials i serveis equivalents

És la portabilitat que coneixíem però ampliada a les xarxes socials.



Il·lustració 20. Portabilitat en xarxes socials. Elaboració pròpia.

11. Dret al testament digital

Es tracta del dret a elaborar un testament amb instruccions específiques per als perfils de les xarxes socials, continguts al núvol, etc. Generà certa polèmica ja que alguns notaris indiquen que no calia modificar-hi la norma. D'altra banda, a la Comunitat Autònoma Catalana això ja es portava a cap mitjançant una modificació del seu Codi Civil. Es concedeix als familiars d'un finat la possibilitat de tenir accés a les dades referents a la seua vida digital si ho sol·liciten, i el difunt no deixara de manera expressa la seua idea en sentit contrari. Si no és així, podran accedir "les persones vinculades al finat per raons familiars", així com modificar o esborrar les dades que continguen. També podran decidir eliminar-ne els perfils de xarxes socials.

Polítiques d'impuls dels drets digitals.

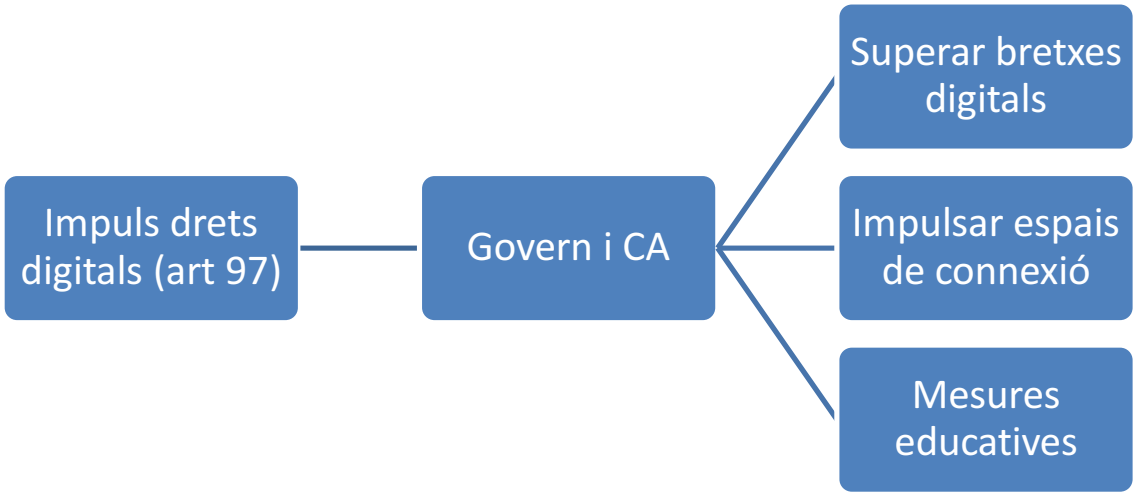
Finalment, es tracta de cobrir una sèrie d'objectius:

a) superar les bretxes digitals i garantir l'accés a Internet de col·lectius vulnerables o amb necessitats especials i d'entorns familiars i socials econòmicament desafavorits mitjançant, entre altres mesures, un abonament social d'accés a Internet;

b) impulsar l'existència d'espais de connexió d'accés públic, i

c) fomentar mesures educatives que promoguen la formació en competències i habilitats digitals bàsiques a persones i col·lectius en risc d'exclusió digital i la capacitat de totes les persones per a realitzar un ús autònom i responsable d'Internet i de les tecnologies digitals.

També es promouran les accions de formació, difusió i conscienciació necessàries per a aconseguir que els menors d'edat facen un ús equilibrat i responsable dels dispositius digitals i de les xarxes socials i dels serveis de la societat de la informació.



Il·lustració 21. Impuls dels drets digitals. Elaboració pròpia.

Breu aproximació ètica al tractament de dades

No pensem que per viure en un moment de màxima eclosió tecnològica estem reinventant normes ètiques i morals. Per a mostra, n'hi ha prou amb fixar-nos en una frase (d'un llibre de 1939!) que sembla escrit per a nosaltres avui mateix:

> *Una cosa és, si més no, clarísima: que les condicions de tot ordre, socials, econòmiques, polítiques, en què treballarà demà són summament distintes de les que treballà fins ara.*
>
> *No parlem, doncs, de la tècnica com si fora l'única cosa positiva, l'única realitat incommovible de l'home. Això és una estupidesa, i com més ofuscats hi estiguen els tècnics, més probable és que la tècnica actual se'n vaja en orri i periclite.*
>
> *N'hi ha prou que canvie un poc substancialment el perfil de benestar que plana davant de 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 pete, es desconjunte i prenga uns altres rumbs.(Ortega y Gasset, 1968)

No, no hi ha res nou sota el sol. Però hi ha elements que produeixen interferències amb la nostra visió clàssica, de segles. Hobbes, en el seu *Leviatan* (Hobbes, 2003) establia un fet que havia sigut acceptat per tothom: el pacte de la ciutadania amb l'estat per la seua seguretat. Aquest 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 aquestes la nostra seguretat, tant en la societat en xarxa com fora d'aquesta. I com és aquest contracte? Qui ha de vigilar les clàusules? Som conscients que en moltes ocasions regalem les nostres dades als nostres proveïdors com Faust venia la seua ànima al diable?

Dèiem que no estàvem inventant 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 la IEEE (Institute of Electrical and Electronics Engineers, una associació tremendament implicada en l'ètica de les TIC), el 1995 aparegué l'important en grandària i continguts *Ethics and Computing* (Bowyer, 1995), on la privacitat ocupa un espai de molt d'interès, i amb una visió que podríem anomenar actual: partint del que ell considera un precedent, les escoltes en línies telefòniques[16] arriba al que denomina *Efecte Gran Germà*, en què busca la resposta en aquell moment únicament en la tecnologia, atès que la parca legislació estatunidenca poca resposta podia donar-hi. En concret, se centra en l'encriptació, en la clau privada[17]. A aquest respecte, resulta interessant llegir, pel contrast, la sentència del Tribunal Suprem, Sala Penal, 1942/2016, on s'avalen les escoltes per mitjans tecnològics, inclosa la utilització dels telèfons mòbils com micròfons ambientals (Recurso de casación por infracción de preceptos constitucionales e infracción de Ley, 2016) . Sobre els estudis tècnics, destaquem (Landau, y otros, 1994) i (Barlow , 1993). Sobre l'espionatge sistemàtic de l'estat (Oltra Gutiérrez, 2001).

D'una banda, proclamem els drets humans, entre els 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 només un número per a un banc, un nom i cognoms substituïbles pel número del DNI. Som tot el que té el fisc de nosaltres, tot el relacionat al nostre carnet de conduir, el nostre historial de la Seguretat Social…, les vegades que hem consultat una cartellera de cine, 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-hi espectres econòmics, sumant-los a informes teus que estan dispersos, fins i tot antics, com ara els teus antecedents patològics familiars, les dades de la teua gestació, àdhuc rumors sobre el teu caràcter. Som, en si, un gegantí i voraç banc de dades on caben tots els fets i les dites de la teua vida (Vázquez & Barroso , 1992)

[16]Des de 1928 es coneixen les intervencions de línies telefòniques per la policia per a lluitar contra el crim. La seua evolució és lenta, però constant. El 1968 es registren als Estats Units unes 900 escoltes realitzades legalment per la policia. Poc després, el mateix concepte es trasllada a les converses via Internet amb detectors legals, per exemple.

[17] Cal que ens faça pensar això per què les aplicacions que se serveixen de PGP, com ara encriptació, tenen problemes transfronterers en considerar-los el legislador de l'altra banda de l'oceà armes.

Dia a dia, voluntàriament o involuntàriament, facilitem a grans bases de dades informació sobre els nostres desigs, les nostres creences i ideologies, i deixem 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 ecos de Foucalt (Foucalt, 2012), l'efecte del panòptic, on fiquem un pres en una cel·la permanentment vigilada, que assegura així el funcionament automàtic del poder, ja que el presoner se sap contínuament observat. La conclusió obvia 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 creixent demanda de seguretat i amb aquesta la necessitat de vigilància; i, d'altra banda, els efectes que la dita 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 altrament, si desitgem viure en una societat justa, sense abusos, on les normes es respecten, lliurement i on un poderós pel simple fet de ser-ho no "valga més" que un d'humil, necessitem bons professionals. Bons, en doble sentit: bons perquè es posseeix un domini excel·lent de la tècnica i bons com a persones, que són capaces de mirar-se a l'espill sabedores que enfront no tenen ningú que trenca l'ètica i la deontologia professional. Perquè si només som bons com a tècnics, i menystenim les normes de comportament, estem llançant al contenidor la part més important de la nostra humanitat i col·locant cunyes per a trencar la nostra societat.

Òbviament, si plantejàrem a classe de manera oberta la pregunta: Què és una persona bona?, eixirien tantes respostes com alumnes. No, no n'hi ha, almenys soc incapaç de donar-la jo, una resposta única a aquesta pregunta. Hi ha moltíssimes consideracions a ser tingudes 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 respecte al tema, hi ha opinions divergents, àdhuc en l'àmbit judicial. Com la recent sentència del Tribunal Europeu de Drets Humans que condemna Espanya a indemnitzar cinc caixeres que furtaven al seu ocupador per vulnerar el dret a la seua privacitat en ser enregistrades amb càmeres ocultes o l'habilitació de cessió a l'Agència Tributària per 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 antics com la humanitat. Aquesta combinació entre ètica, llei, decisions personals i decisions polítiques ens acompanyen des de l'antic Egipte, des dels codis primitius, on ja s'al·ludeix a raons morals. En el cas de la privacitat, des de l'article de (Warren & Brandeis, 1890) es llegeix per molts com un dret moral a ser protegit per la llei[18]. Per organitzar un poc les idees, i seguint (Colmenarejo Fernández, 2017), enumerarem unes raons morals per a la protecció de les dades personals:

[18] Podem pensar, sense anar més lluny, en la tan usada per les pel·lícules de Hollywood Quarta Esmena, de 1789, text aprovat definitivament per Jefferson el 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 perquè les seues persones, domicilis, papers i efectes estiguen estàlvies de*

- Prevenció de danys. Per exemple, garantint que les contrasenyes d'accés són segures, o que la geolocalització no és activada pels 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 enfront d'empreses o governs. Les lleis tenen per 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 implicar discriminació. La informació personal proporcionada en un context (p. e. durant una anàlisi mèdica) pot canviar-ne el significat en un altre context (p. e. en processos de contractació o en transaccions comercials[19]) 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 seues eleccions. Pensem en les notícies falses que donen suport a un candidat enfront d'un altre, que aconsegueixen ser les més difoses. Es mostren a més aquells usuaris que poden estar potencialment d'acord, que ens porten 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 es permeta corregir inexactituds.

Solem trobar reticències. És habitual al·ludir a la neutralitat de les dades i de la tecnologia per a justificar l'innecessari 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 gran grandària i el cada vegada major nombre provoquen canvis en les activitats relacionades amb la nostra identitat. La societat, a vegades de forma imperceptible, pateix canvis en la valoració del que és la privacitat, que implica controlar dades d'altres i només es desperta davant d'elements crítics, com ara la necessitat de gestionar la nostra reputació. (Colmenarejo Fernández, 2017)

Podríem adduir una suposada objectivitat dels mètodes quantitatius. Aquesta suposada objectivitat es fonamenta en la forma que tenen els sistemes d'informació d'eludir o evitar la intervenció humana. Això vindria a afermar aquests paradigmes que ens parlen del determinisme tecnològic. Hem d'assumir que els atributs tècnics de la tecnologia han de ser analitzats socialment i èticament, i no només tècnicament, ja que les innovacions tecnològiques lluny de ser neutrals sempre estan orientades cap un fi polític. (Colmenarejo Fernández, 2017). A més, avui, amb el *núvol*, la dispersió de servidors al llarg del globus, que ens fa concebre les bases de dades com un *objecte* sense un entorn físic, ens provoca un distanciament extra en la moralitat. Ens recorda Colmenarejo una cita d'Aranguren, segons la

---

perquisicions i d'aprehensions arbitràries serà inviolable, i no s'expediran a aquest efecte manaments que no tinguen un motiu versemblant, estiguen corroborats mitjançant jurament o protesta i descriguen amb particularitat el lloc que ha de ser registrat i les persones o coses que han de ser detingudes o embargades."

[19]Com justifiquem la correlació de dades entre la informació d'un historial sanitari d'un ciutadà amb la informació sobre les seues cerques a Google? Recordem webs com ara <PatientsLikeMe> (Patients Like Me), d'on es furtaren dades per a la venda a companyies sanitàries. Això hauria de fer-nos reflexionar, entre d'altres, sobre la relació de l'exportació de dades amb la portabilitat com a nou dret de protecció de dades.

qual davant d'un estímul els humans hem de conformar necessàriament la realitat abans de prendre una decisió, hem de parar-nos a pensar, detenir-nos a justificar la nostra acció davant d'un ventall de possibilitats que s'ubica en la irrealitat. Diu Aranguren que la primera dimensió de la llibertat de les persones es dona precisament en aquest alliberar-se de l'estímul que suposa la reflexió. La segona dimensió de la llibertat que no es és pròpia es fa efectiva quan prenem una decisió, quan decidim actuar d'un manera i no d'una altra, quan justifiquem els nostres actes està la dimensió moral, que ens és inherent a tots els éssers humans, la nostra capacitat per a decidir-nos entre irrealitats possibles i distingir entre bé, malament i o allò que atén exclusivament els nostres interessos. I dit això: Com conformem una realitat *no tangible*?

Sembla, doncs, 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 en (De la Cueva, 2018) per a desmuntar això. D'una banda, les solucions donades pels sistemes informàtics a unes necessitats de gestió de la informació no tenen cap suport jurídic, són meres interpretacions d'un humà, el que va construir aquell algorisme. Això trenca en mil trossos la idea de la neutralitat de la tecnologia. És més; ens converteixen en presos d'unes imposicions tècniques que no admeten la seua discussió, ja que es mostren com irrebatibles, fet que ens porta a una verdadera dictadura de la màquina. Ens queda pendent, permeteu-me el joc de paraules, el vaporós assumpte del núvol. Que no és tant, perquè que no veiem les màquines no significa que aquestes no estiguen i, per tant, queden lliures de subjeccions legals o morals.

No fa tant se'ns deia que a Internet podíem passar pel que volguérem. Una *top model*, un camioner rude, un infant, un actor o un amant de les foques. Avui, 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 les fem, quantes vegades hem anat a veure-les i què n'hem escrit. Fins i tot quina roba portàvem quan hi escrivíem. Com es construeixen aquests registres? Quina transparència té el ciutadà d'aquests? Hi ha un seguit de problemes sobre això que (Colmenarejo Fernández, 2017) enumera:

- Els usuaris no han arribat a comprendre com afecten aquestes violacions de privacitat tant individus com el 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 poden ser compartides a vegades de forma automàtica. Això dificulta que els usuaris puguen exercir-ne el dret a corregir errors o falsedats que els afecten mitjançant un adequat procediment.
- Possibilitat de programar anàlisis que permeten predir amb exactitud de manera automàtica un ampli rang d'atributs sensibles com, p. e., l'orientació sexual, creences religioses, ideologia política, ús de drogues, test intel·ligència, etcètera.
- Desajust de les polítiques reclamades pels 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[20].

[20] És d'interès visualitzar el documental *Pre-Crimen* (Hielscher & Heeder, 2018)

- 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 constitueix llavors un acte creatiu? Caldria parlar del dret a la propietat de les dades parlant de la lliure exposició d'aquests per a fer-ne l'ús de la forma que considerem. El desafiament arriba en tractar l'espinós tema de la publicitat actual, directa cap a nosaltres amb les dades que conscientment moltes vegades les hem donat. Això és, potser cal protegir-nos de nosaltres mateixos, mitjançant tecnologia aquesta dissenyada amb requisits de privacitat en el programari i el maquinari. Per a fer més còmode això, (Colmenarejo Fernández, 2017) proposa una taxonomia de la privacitat d'acord amb els diferents moments:

1. Recol·lecció: vigilància i interrogació amb objecte 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 avui 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

Acabem de veure com, en tota actuació professional, no només n'hi prou amb 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 uns camins adequats es converteix en un fet, més que important, quasi imprescindible. Així, el Reglament incita associacions que representen responsables o encarregats perquè elaboren codis de conducta[21], a fi de facilitar-ne l'aplicació efectiva i interpretar les característiques específiques en cada sector i les necessitats específiques, sobretot, de les pimes.

En aquests codis és d'interès establir les obligacions dels responsables i encarregats.

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

Alguns elements a considerar en aquests codis:

[21] Podem enllaçar això amb els criteris per a la construcció de codis deontològics o de bona pràctica professional, en què 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 intervenen en el tractament o ús de dades personals.
• Les garanties per a l'exercici dels drets de les persones afectades.

1. el tractament lleial i transparent;
2. els interessos legítims perseguits pels responsables;
3. la recollida 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 infants i la protecció d'aquests;
8. la notificació de violacions de la seguretat de les dades personals
9. la transferència de dades personals a tercers països

Les associacions i altres organismes que projecten elaborar un codi de conducta o modificar o ampliar un codi existent presentaran 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 és aprovat, l'autoritat de control registrarà i publicarà el codi. El Comitè arxivarà en un registre tots els codis de conducta, modificacions i ampliacions que s'aproven i els posarà 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 disposa en aquest Reglament 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 oferides pels responsables o encarregats no subjectes a aquest Reglament. Aquesta certificació serà voluntària i estarà disponible a través d'un procés transparent. S'expedirà a un responsable o encarregat de tractament per un període màxim de tres anys i podrà ser renovada en les mateixes condicions, sempre que se seguisquen complint els requisits pertinents. La certificació serà retirada, quan no es complisquen o s'hagen deixat de complir els requisits per a la certificació.

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

Els organismes de certificació que siguen acreditats per l'autoritat de control, per 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 per ambdós. Aquesta acreditació s'expedirà per un període màxim de cinc anys i podrà ser renovada en les mateixes condicions.

Situació i conclusions

L'ésser humà sembla 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 gran confusió. Llegim en la premsa dades sorprenents i titulars encara més cridaners que ens fan pensar que les empreses semblen dividir-se entre les que s'han

assabentat que hi ha una legislació europea de protecció de dades i intenten fer alguna cosa, amb divers èxit, i els que encara *passen*, per no parlar de casos pitjors (recordem l'assumpte de Cambridge Analytica amb les dades preses de Facebook).

Cal tenir en compte la dificultat d'harmonitzar en una legislació les 27 precedents dels distints països de la Unió, alhora que vigilar que els canvis produïts per aquesta es porten a cap de forma raonable. Tots rebem al seu moment una pluja de peticions de consentiment que, alhora 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.

Hem vist molts aspectes canviants a considerar, aspectes a ser tamisats per la Llei 3/2018, per exemple, sobre l'espinós tema dels difunts, en facilitar que els hereus puguen dirigir-se al responsable de tractament, excepte si el finat no va dir una altra cosa o hi ha una llei que ho impedisca. També apareixen canvis respecte als menors (menors, els seus tutors o el Ministeri Fiscal; igual per a discapacitats menors) on es rebaixa l'edat crítica de 14 a 13 anys.

Aquest tipus de legislació és susceptible de rebre molts canvis, bé per la promulgació de noves lleis, directives…, bé per la correcció de les actuals (per exemple,(Europea, 2018)). És molt important per al professional no abaixar-hi la guàrdia.

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

Un punt d'interès per a aquest el tenim en les memòries anuals de l'AEPD.

Un exemple de pròxima actualització el tenim amb el "i-privacy".(Comisión 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, que regula aspectes com ara 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 de 2009 s'estan donant passes per a substituir-la, aquesta vegada com a Reglament, per a evitar problemes a l'hora d'execució simultània en els distints països de la Unió. Alguns dels aspectes a renovar és la millora dels navegadors pel que fa a la protecció de dades, ja que ha de deixar d'importar el dispositiu des del qual s'empre. És un fet que entra en l'anomenada privacitat per disseny i que busca que els usuaris no hagen de visitar innumerables i canviants menús per a protegir-ne les dades. També apareixen regles estrictes per a les galetes.

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 d'aquesta, podrem accedir als cercadors d'AENOR, per a normes tècniques, i ARANZADI, on destaca el seu arxiu de jurisprudència.

Eines de l'AEPD (Facilita, avaluació d'impactes, anàlisis de riscos…): disponibles a: https://gestiona.aepd.es/

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(GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS, 2017)
- Orientacions de la Comissió sobre l'aplicació directa del Reglament general de protecció de dades: (Comisión 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, 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 (CEE) n339/93(PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA, 2008)
- Requisits per a organismes que certifiquen productes, processos o serveis (AENOR, 2012)

Altres textos d'interès:

Per a aprofundir en determinats temes:

- AGPD: Procediment per incorporació a un grup de Whatsapp (Agencia Española de Protección de Datos, 2017)
- AGPD: Procediment per transmissió de fotos per Whatsapp (Agencia Española de Protección de Datos, 2017)
- AGPD: Procediment sancionador contra Google Street View (Agencia Española de Protección de Datos, 2017)
- Circular del Ministeri Fiscal sobre intervenció de comunicacions electròniques (FISCALÍA GENERAL DEL ESTADO, 2013)
- Dret a l'oblit. Cas Mario Costeja: (Google vs Mario Costejá, 2014)
- El Tribunal d'Apel·lació dels Estats Units declara que els *likes* de Facebook estan protegits per la Primera Esmena: (Bland vs Roberts, 2013)
- Llibertat d'informació, dret a la pròpia imatge i autocensura dels mitjans: (Salvador, Rubí, & Ramírez, 2011)
- Menors a internet: (Davara Fernández de Marcos, Madrid)
- Sentència: dret a l'oblit digital: (Derecho al olvido digital. Digitalización de hemeroteca sin utilizar códigos ni instrucciones que..., 2015)
- Sobre l'ús de càmera oculta: Tesi doctoral (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 al Registre General

Resposta correcta: b). 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 serien

a) Cessió, tractament i utilització
b) Recollida, dissociació i utilització
c) Recollida, tractament i utilització
d) Recollida, tractament i portabilitat

Resposta correcta: c). Pàgina 14

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

a) La rectificació de les dades personals inexactes que li concernisquen
b) La dissociació de les dades personals inexactes que li concernisquen
c) La dissociació de les dades personals exactes que li concernisquen
d) Totes les anteriors són correctes

Resposta correcta: a). Pàgina 19

Fa falta un delegat de protecció de dades

a) Si es tracta d'un tractament des de l'Administració pública
b) Quan es treballa amb dades d'un elevat nombre de persones
c) Quan es treballa amb un elevat nombre de dades especials
d) Totes les anteriors són correctes

Resposta correcta: d). Pàgina 25.

ANNEX. Actuacions tècniques del professional.

Tractarem en aquest apartat els elements de més importància per al professional. Ens focalitzarem en l'avaluació d'impacte, i deixarem per a millor ocasió un desenvolupament de la necessitat d'establir mitjançant contracte l'obligació de l'anàlisi de riscos i altres tasques importants, com ara portar a cap el registre d'activitat o notificar violacions de seguretat i les elementals de garantia de la seguretat de les dades tractades i cooperació amb l'autoritat de control. Elements com són l'aplicació de la portabilitat amb les conseqüents derivades d'ús de

formats estructurats d'ús comú, de lectura mecànica…, han de quedar al bon saber i fer del professional.

Avaluació d'impacte (EIPD)

Es tracta d'avaluar de manera anticipada quins són els potencials riscos a què estan exposades les dades personals en funció de les activitats de tractament que es porten a cap amb aquestes. Una EIPD és un procés utilitzat per a reforçar i demostrar el compliment.

De forma òbvia, això implica una anàlisi de riscos, el qual permet identificar els riscos que planen sobre les dades dels interessats i establir una resposta que adopte les salvaguardes necessàries per a reduir-los fins un nivell de risc acceptable.

El RGPD preveu que les avaluacions d'impacte es porten a cap "abans del tractament". Hi ha un parell de documents imprescindibles per al professional. D'una banda, la Guia que l'AEPD publicà (AEPD, 2017) i, de l'altra, les directrius que sobre l'EIPD va donar el Grup de l'Article 29 (Grupo "Protección de datos" del artículo 29, 2017). De l'altra, i per al moment concret de la notificació de bretxes de seguretat, recordem que també hi ha una guia sobre això (AEPD & INCIBE, 2017).

Quan s'ha de fer?

L'avaluació d'impacte s'ha de portar a cap quan siga probable que un tipus de tractament per la seua naturalesa, abast, context o fins comporta un alt risc per als drets i llibertats de les persones físiques.

Si en realitzar-la es veu que el tractament implicaria un alt risc si el responsable no pren mesures per a mitigar-lo.

Per a determinar si és necessari portar a cap l'avaluació d'impacte o no, es pot seguir una breu metodologia d'anàlisi en dues fases (art. 35. RGPD), (art. 28 Llei 3/2018):

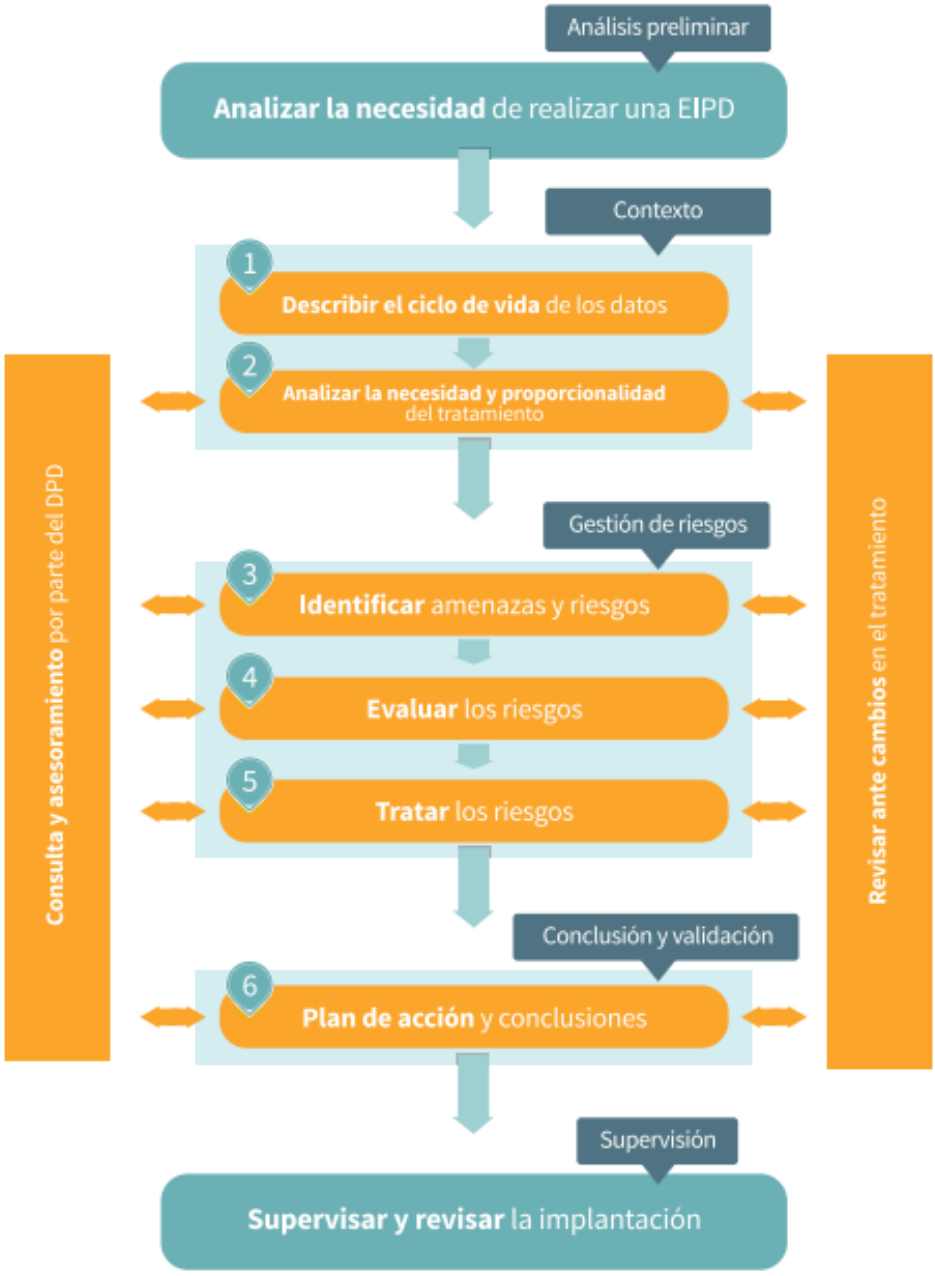
Fase 1. Analitzar les llistes de tractaments previstos en la regulació;

1.1) Avaluació sistemàtica i exhaustiva d'aspectes personals de persones físiques que es base en un tractament automatitzat, com ara l'elaboració de perfils, i sobre la base del qual es prenen decisions.

1.2) Tractament a gran escala de les categories especials de dades o de les dades personals relatives a condemnes i infraccions penals.

1.3) Observació sistemàtica a gran escala d'una zona de accés públic.

Fase 2. Anàlisi de la naturalesa, abast, context i fins de tractament: si s'utilitzen TIC o si per la seua naturalesa, abast, context o fins comporte un alt risc per als drets i llibertats de les persones físiques.



Il·lustració 22. Flux a seguir en una EIPD. Font: AEPD, guia pràctica per a les EIPD

Què ha d'incloure com a mínim?

1. Descripció sistemàtica de les operacions de tractament previstes, dels fins d'aquest i, si pertoca, l'interès legítim perseguit pel responsable del tractament.

2. Avaluació de la necessitat i la proporcionalitat de les operacions de tractament amb respecte a la seua finalitat.

3. Avaluació dels riscos per als drets i llibertats dels interessats.

4. Mesures previstes per a afrontar els riscos, demostrant la conformitat amb el Reglament General.

Mesures pal·liatives que determine l'autoritat de control

Hi ha la necessitat d'adoptar les mesures pal·liatives o correctives del tractament pretès, quan aquest porte amb si un alt risc de vulneració dels drets i llibertats dels interessats o titulars de les dades, en busca de minvar els riscos i, si és el cas, els perjudicis que, si es produeixen, s'hagueren pogut originar als titulars de les dades, si els tractaments s'hagueren portat a cap de manera efectiva.

Són mesures correctores o moderadores del risc. Moltes vegades la gravetat de l'impacte es pot evitar amb un disseny millor d'aquest. Totes aquestes actuacions hauran de quedar incorporades i acreditades documentalment en les subcarpetes corresponents d'aquesta carpeta, als efectes de la constància deguda.

Quins criteris adoptar?

a) Reduir al màxim el tractament de dades personals.

b) Pseudoanonimitzar com més prompte millor les dades personals.

c) Donar transparència a les funcions i el tractament de dades personals.

d) Permetre als interessats supervisar el tractament de dades.

i) Crear i millorar elements de seguretat.

A més, aquells criteris que l'AEPD indica: Licitud, lleialtat i transparència; Limitació de la finalitat (les dades es recullen amb un fi determinat); Minimització de dades; Exactitud; Limitació del termini de conservació; Integritat i confidencialitat.

Directrius del Grup 29

En aquest apartat tractarem de resumir els aspectes més importants de l'imprescindible document ja esmentat *Directrius sobre l'avaluació d'impacte relativa a la protecció de dades (EIPD) i per a determinar si el tractament «comporta probablement un alt risc» a efectes del Reglament (UE) 2016/679* (Grupo "Protección de datos" del artículo 29, 2017). El resum és més que això: és una síntesi de paràgrafs destacats de la guia, de què recomanem encaridament la lectura i estudi.

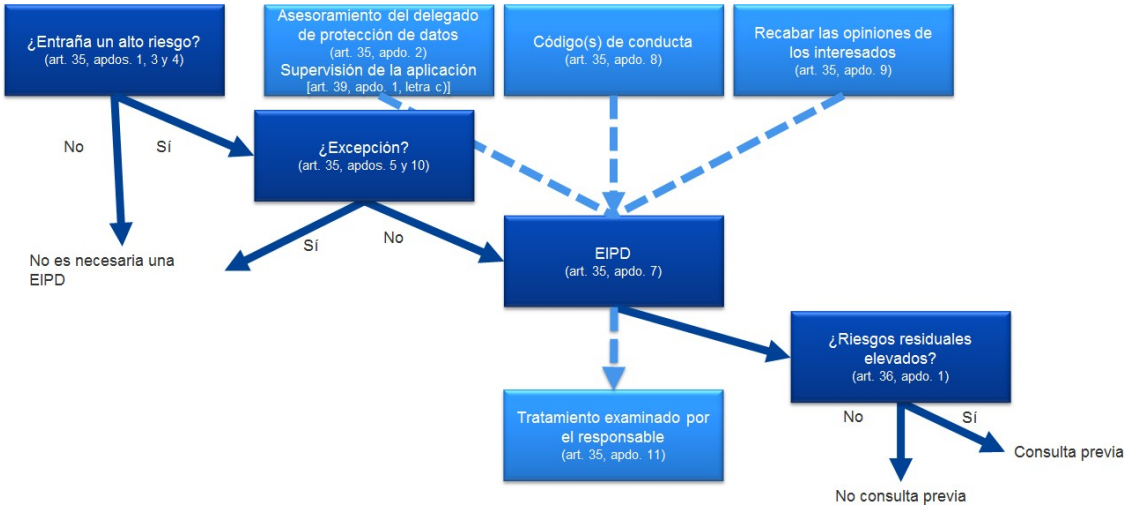
Comencem definint què és un risc i la seua gestió.

Un *risc* és un escenari que descriu un esdeveniment i les seues conseqüències, estimat en termes de gravetat i probabilitat. La *gestió de riscos* es pot definir com les activitats coordinades per a dirigir i controlar una organització respecte del risc. Per a nosaltres aquesta lectura va tamisada per l'article 35 del RGPD, que es refereix a un probable alt risc «per als drets i llibertats de les persones». En aquesta referència «als drets i llibertats» dels interessats no solament s'apunta als drets a la protecció de dades i a la intimitat, sinó a altres drets fonamentals, com ara la llibertat d'expressió, la llibertat de pensament, la llibertat de circulació, la prohibició de discriminació, el dret a la llibertat i la llibertat de consciència i de religió.

L'AEPD té una guia magnífica molt recomanable, la *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al AEPD* (AEPD, 2017), d'on traiem aquesta imatge:

Il·lustració 23. Riscos i la seua gestió. Font: Guía práctica de análisis de riesgos...

La guia del Grup 29 ens mostra una altra imatge molt aclaridora.



Il·lustració 24. Principis bàsics relacionats amb l'EIPD en el RGPD . Font: Directrices...

Anirem responent, seguint mil·limètricament la guia, les preguntes més importants.

Què aborda una EIPD? Una única operació de tractament o un conjunt d'operacions de tractament similars?

Es pot utilitzar una única EIPD per a avaluar múltiples operacions de tractament que siguen semblants en termes de naturalesa, abast, context, fins i riscos. Un exemple: es pot per a una companyia de ferrocarrils cobrir-ne la videovigilància de totes les estacions amb només una EIPD. Això seria igualment aplicable a operacions de tractament semblants aplicades per diversos responsables.

Una EIPD també pot servir per a avaluar l'impacte relatiu a la protecció de dades d'un producte tecnològic, de tal manera que el responsable del tractament que instal·la el producte continua tenint l'obligació de portar a cap la pròpia EIPD relativa a l'aplicació específica, però aquesta es pot basar en una EIPD preparada pel proveïdor del producte.

Quines operacions de tractament s'han de sotmetre a una EIPD?

Tret d'excepcions, totes les que «probablement comporten alt risc». Llevat que l'operació de tractament complisca una excepció, s'ha de realitzar una EIPD quan una operació de tractament «comporte probablement un alt risc».

Quan resulta obligatòria una EIPD? Quan el tractament «comporte probablement un alt risc». En els casos que no estiga clar si es requereix una EIPD, el GT29 recomana realitzar-ne una.

Per a entendre quin conjunt d'operacions de tractament requeririen una EIPD atès el seu alt risc inherent, s'han de considerar els nou criteris següents:

1. Avaluació o puntuació, inclosa l'elaboració de perfils i la predicció, especialment d'«aspectes relacionats amb el rendiment en el treball, la situació econòmica, la salut, les preferències o interessos personals, la fiabilitat o el comportament, la situació o els moviments de l'interessat». Alguns exemples d'això podran incloure una institució financera que investigue els seus clients en una base de dades de referència de crèdit o en una base de dades contra el blanqueig de capitals i el finançament del terrorisme o sobre fraus.

2. Presa de decisions automatitzada amb efecte jurídic significatiu o semblant: tractament destinat a prendre decisions sobre els interessats que produeix «efectes jurídics per a les persones físiques» o que les afecten «significativament de manera similar». Per exemple, el tractament pot provocar exclusió o discriminació contra les persones.

3. Observació sistemàtica: tractament usat per a observar, supervisar i controlar els interessats, incloses les dades recollides a través de xarxes o «observació sistemàtica [...] d'una zona d'accés públic»

4. Dades sensibles o dades molt personals: això inclou les categories especials de dades personals definides en l'article 9 (per exemple, informació sobre les opinions polítiques de les persones), així com dades personals relatives a condemnes i infraccions penals segons la definició de l'article 10. Un exemple seria un hospital general que guarda historials mèdics de pacients o un investigador privat que guarda dades de delinqüents.

5. Tractament de dades a gran escala: determinar si el tractament es realitza a gran escala:

5.1. El nombre d'interessats afectats, bé com a xifra concreta o com a proporció de la població corresponent;

5.2. El volum de dades o la varietat d'elements de dades distintes que es processen;

5.3. La durada, o permanència, de l'activitat de tractament de dades;

5.4. L'abast geogràfic de l'activitat de tractament.

6. Associació o combinació de conjunts de dades, per exemple procedents de dues o més operacions de tractament de dades realitzades per a distints fins.

7. Dades relatives a interessats vulnerables:

8. Ús innovador o aplicació de noves solucions tecnològiques o organitzatives, com ara combinar l'ús d'empremta dactilar i reconeixement facial.

9. Quan el mateix tractament «impedeix als interessats exercir un dret o utilitzar un servei o executar un contracte». Un exemple d'això seria quan un banc investiga els seus clients en una base de dades de referència de crèdit a fi de decidir si els ofereix un préstec.

En la majoria dels casos, un responsable del tractament pot considerar que un tractament que compleix dos criteris requerirà la realització d'una EIPD. Tanmateix, en alguns casos, un responsable del tractament pot considerar que un tractament que en compleix només un requereix una EIPD.

Exemples sobre com avaluarem si una operació de tractament concreta requereix una EIPD:

Exemple	Criteris	EIPD necessària?
Hospital que tracta les dades genètiques i sanitàries dels seus pacients.	Dades sensibles o dades molt personals. Dades relatives a interessats vulnerables. Tractament de dades a gran escala.	SÍ
Sistema de càmeres en autovies. Hi ha un sistema intel·ligent per a seleccionar cotxes i reconèixer matrícules.	Observació sistemàtica. Ús innovador o aplicació de solucions tecnològiques o organitzatives.	SÍ
Observació d'activitats d'empleats: lloc de treball, Internet…	Observació sistemàtica. Dades relatives a interessats vulnerables.	SÍ
Recollida de dades dels mitjans socials públics per a elaborar perfils.	Avaluació o puntuació. Tractament de dades a gran escala. Associació o combinació de conjunts de dades. Dades sensibles o dades molt personals	SÍ
Base de dades nacional de qualificació creditícia o sobre fraus.	Avaluació o puntuació. Presa de decisions automatitzada amb efecte jurídic significatiu o similar. Impedeix als interessats exercir un dret o	SÍ

	utilitzar un servei o executar un contracte. Dades sensibles o dades molt personals.	
Dades personals de pacients o clients per un sol metge, un altre professional de la salut o advocat.	Dades sensibles o dades molt personals. Dades relatives a interessats vulnerables.	NO
Revista en línia que use una llista de distribució per a enviar un resum diari .	Tractament de dades a gran escala.	NO
Web de comerç electrònic que mostra anuncis de peces de cotxes clàssics que suposa una elaboració de perfils limitada basada en elements vistos o adquirits al seu lloc web.	Avaluació o puntuació.	NO

No es requereix una EIPD en els casos següents:

- quan «no siga probable que el tractament comporte un alt risc per als drets i llibertats de les persones físiques»;

- quan la naturalesa, l'abast, el context i els fins del tractament siguen molt similars al tractament per al qual s'ha realitzat l'EIPD;

- quan les operacions de tractament hagen sigut comprovades per l'autoritat de control abans de maig de 2018 en condicions específiques que no hagen canviat;

- quan una operació de tractament tinga una base jurídica en el Dret de la Unió o en el Dret de l'Estat membre i quan ja s'haja realitzat una EIPD;

- quan el tractament s'incloga en la llista opcional (establida per l'autoritat de control) d'operacions de tractament per als quals no es requereix una EIPD.

Què passa amb les operacions de tractament ja existents?

El requisit de realitzar una EIPD s'aplica a operacions de tractament existents que probablement comporten un alt risc per als drets i llibertats de les persones físiques i per a les que s'ha produït un canvi dels riscos, tenint en compte la naturalesa, l'abast, el context i els fins del tractament. Per raó de bones pràctiques, una EIPD ha de ser contínuament revisada i reavaluada amb regularitat.

Com s'ha de portar a cap una EIPD?

Moment: abans del tractament. L'EIPD s'ha d'iniciar tan prompte com siga viable en el disseny de l'operació de tractament, fins i tot encara que algunes de les operacions de tractament no es coneguen encara. Portar a cap una EIPD és un procés continu, no una mesura excepcional.

Consell: resulta una bona pràctica definir i documentar altres funcions i responsabilitats específiques. Per exemple:

- en el cas que unitats empresarials específiques proposaren portar a cap una EIPD, les dites unitats haurien d'aportar informació a l'EIPD i participar en el procés de validació de la dita avaluació;

- si és el cas, es recomana sol·licitar l'assessorament d'experts independents de distintes professions (advocats, experts en TI, experts en seguretat, sociòlegs, experts en ètica, etc.).

- les funcions i responsabilitats dels encarregats del tractament s'han de definir contractualment.

- el responsable principal de la seguretat de la informació (CISO), en cas de ser nomenat, així com el delegat de protecció de dades, podrien suggerir que el responsable portara a cap una EIPD sobre una operació de tractament específica, i haurien d'ajudar les parts interessades en la metodologia, ajudar a avaluar la qualitat de l'avaluació de risc i si el risc residual és acceptable, i a desenvolupar coneixements específics per al context del responsable del tractament;

Quina és la metodologia per a portar a cap una EIPD?

El RGPD estableix les característiques mínimes d'una EIPD (Article 35, apartat 7, i considerants 84 i 90). En la guia s'ofereix un gràfic que il·lustra el procés iteratiu genèric per a realitzar una EIPD:

Il·lustració 25. Procés iteratiu genèric per a realitzar una EIPD. Font: Guía...

Hi ha una sèrie de components de l'EIPD que se superposen amb components ben definits de gestió del risc (p. e., ISO 31000). Hi ha un seguit de marcs relatius a l'EIPD a la Unió Europea que cal considerar[22].

[22] **Exemples de marcs genèrics de la UE:**
- DE: Standard Data Protection Model (model estàndard de protecció de dades), V.1.0 – versió de prova, 2016. https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia Española de Protección de Datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

- FR: Privacy Impact Assessment (PIA) (avaluació d'impacte relativa a la intimitat), Commission nationale de l'informatique et des libertés (CNIL), 2015. https://www.cnil.fr/fr/node/15798
- UK: Conducting privacy impact assessments code of practice (realització d'avaluacions d'impacte relatives a la intimitat: codi de pràctica), Oficina del Comisario de Información (ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Exemples de marcs de sectors específics de la UE:
- Privacy and Data Protection Impact Assessment Framework for RFID Applications (marc d'avaluació d'impacte relatiu a la intimitat i la protecció de dades per a les aplicacions RFID). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Model d'avaluació de l'impacte sobre la protecció de dades per a xarxes intel·ligents i per a sistemes de comptador intel·ligent http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Això pot provocar un embolic; de fet, es poden usar diferents metodologies per a ajudar a l'aplicació dels requisits bàsics establits en el RGPD. S'han identificat criteris comuns a fi de permetre l'existència d'aquests distints enfocaments, alhora que es permet als responsables del tractament complir amb el RGPD. Aclareixen els requisits bàsics del Reglament, però ofereixen un abast suficient per a les diferents formes d'aplicació. Aquests criteris es poden usar per a mostrar que una metodologia d'EIPD particular compleix els estàndards exigits pel RGPD. Depèn del responsable del tractament elegir una metodologia, però aquesta ha de complir els criteris establits en l'annex 2 de la guia[23].

Així mateix, una norma internacional oferirà directrius sobre les metodologies utilitzades per a portar a cap l'EIPD (ISO/CEI 29134).

[23] **Criteris per a una EIPD acceptable**

El GT29 proposa els criteris següents que els responsables del tractament poden usar per a avaluar si una EIPD, o una metodologia usada per a realitzar una EIPD, és suficientment exhaustiva per a complir amb el RGPD:

- s'ofereix una descripció sistemàtica del tractament
  - es tenen en compte la naturalesa, l'àmbit, el context i els fins del tractament;
  - es registren les dades personals, els destinataris i el període durant el qual es conservaran les dites dades;
  - s'ofereix una descripció funcional de l'operació de tractament;
  - s'identifiquen els mitjans de què depenen les dades personals (maquinari, programari, xarxes, persones, paper o canals de transmissió del paper);
  - es té en compte el compliment dels codis de conducta aprovats;
- s'avaluen la necessitat i la proporcionalitat
  - es determinen les mesures previstes per a complir-lo, tenint en compte:
  - les mesures que contribueixen a la proporcionalitat i la necessitat del tractament sobre la base de:
    - fins determinats, explícits i;
    - legalitat del tractament;
    - dades adequades, pertinents i limitades al necessari;
    - durada limitada de la conservació;
  - mesures que contribueixen als drets dels interessats:
    - informació facilitada a l'interessat;
    - dret d'accés i a la portabilitat de les dades;
    - dret de rectificació i de supressió;
    - dret d'oposició i a la limitació del tractament;
    - relacions amb els encarregats del tractament;
    - garanties concurrents en les transferències internacionals;
    - consulta prèvia;
- es gestionen els riscos per als drets i llibertats dels interessats;
  - s'aprecien l'origen, la naturalesa, la particularitat i la gravetat dels riscos o, més concretament, de cada risc (accés il·legítim, modificació no desitjada i desaparició de dades) des de la perspectiva dels interessats;
    - es tenen en compte els orígens dels riscos;
    - s'identifiquen efectes possibles sobre els drets i llibertats dels interessats en cas que es produïsquen fets que incloguen l'accés il·legítim, la modificació no desitjda o la desaparició de dades;
    - s'identifiquen les amenaces que poden provocar l'accés il·legítim, la modificació no desitjada o la desaparició de dades;
    - s'estimen la probabilitat i la gravetat;
  - es determinen les mesures previstes per a tractar aquests riscos;
- participen les parts interessades
  - se sol·licita l'assessorament del delegat de protecció de dades;
  - es recullen les opinions dels interessats o els seus representants.

No hi ha l'obligació de publicar l'EIPD, però publicar un resum podria fomentar la confiança, i s'ha de comunicar l'EIPD completa a l'autoritat de control en cas de consulta prèvia o si així ho sol·licita l'APD. La publicació d'una EIPD no representa un requisit jurídic del RGPD, ja que és una decisió que correspon al responsable del tractament. Tanmateix, els responsables han de considerar almenys la publicació d'algunes parts, com ara un resum o una conclusió del seu EIPD.

Quan s'ha de consultar l'autoritat de control?

Quan els riscos residuals siguen elevats. Un exemple de risc residual elevat inacceptable inclou casos en què els interessats es poden trobar amb conseqüències importants, o fins i tot irreversibles, de les quals no es poden recuperar (p. e.: un accés il·legítim a dades que supose una amenaça per a la vida dels interessats, un acomiadament, un perill financer) o quan semble obvi que hi haurà un risc (p. e.: per no poder reduir el nombre de persones que accedeixen a les dades a causa dels seus modes d'intercanvi, ús o distribució, o quan no es corregeix una vulnerabilitat coneguda).

Quan el responsable del tractament no puga trobar suficients mesures per a reduir els riscos fins un nivell acceptable (és a dir, els riscos residuals continuen sent elevats), s'ha de consultar l'autoritat de control.

Altres elements d'interès a considerar:

A la manera de calaix de sastre, apareixen elements que no ha de perdre de vista el professional.

Tractament de categories especials.

Parlem d'elements relacionats amb la medicina preventiva o laboral, amb els molt sensibles de salut, política, religió…, i la seua relació amb l'interès públic, i l'assumpte freqüentment oblidat de les condemnes i infraccions penals.

Considerem que hi ha categories de tractament que necessiten una alta especialització, com ara els tractaments amb alt risc, les transferències internacionals de dades, l'elaboració de perfils, la gestió de dades tractades per grups d'empreses o de dades de titularitat o interès públic.

Hi ha una llarga sèrie d'elements recomanables, des de la coneguda guia de l'Agència Catalana de Protecció de Dades per als centres educatius (Agencia Catalana de Protección de Datos, 2018) a normes internacionals, com ara l'ISO/IEC 29187 (Information technology -- Identification of privacy protection requirements pertaining to learning, education and training)

Protecció de dades des del disseny i per defecte

Es tracta d'un fet a preveure abans de determinar el tractament, incloent-hi mesures tècniques i organitzatives. Es pretén quedar-se només amb les dades necessàries.

Exemples:

Protecció de dades des del disseny: mitjançant l'ús de pseudonimització (substitució del material d'identificació personal) i de xifratge (codificació de missatges de forma que només les persones autoritzades puguen llegir-los).

Protecció de dades per defecte: animant una plataforma de xarxes socials a configurar els paràmetres del perfil dels usuaris en l'entorn que més protegisca la intimitat, per exemple limitant des del primer moment l'accessibilitat del perfil dels usuaris perquè per defecte no siga accessible a un nombre indefinit de persones.

Guies i documentació d'alt interès per al professional.

Un element d'alt interès són les avaluacions d'impacte. Per a això, proposem tres elements quasi imprescindibles. D'una banda, la guia de la mateixa AEPD (*Guía práctica para las evaluaciones de impacto en la protección de las datos sujetas al RGPD*) (AEPD, 2017), de l'altra, la més àmplia encara guia de l'Agència Catalana de Protecció de Dades (Avaluació d'impacte relativa a la protecció de dades) (Autoritat Catalana de Protecció de Dades, 2018) i, finalment, l'aplicació *open source* de la CNIL, que podem considerar l'agència francesa. (CNIL, 2019)

Sobre el deure d'informar. A qui, com i quan, incloent-hi la Gestió dels drets: què, com, on, quan…, l'AEPD té una magnífica guia: *Guía para el cumplimiento del deber de informar* (AEPD, 2016).

La responsabilitat del responsable: els contractes amb encarregat, revisió de mesures, polítiques de protecció de dades, corresponsables, autoritzacions prèvies…, podem consultar les directrius per a l'elaboració de contractes entre responsables i encarregats de tractament (AEPD, 2016).

Notificació de bretxes de seguretat. A més de distints formularis de l'AEPD, podem consultar les directrius sobre la notificació de les violacions de la seguretat de les dades personals d'acord amb el Reglament 2016/679 (Grupo de trabajo sobre protección de datos del artículo 29, 2018). També sobre bretxes de seguretat són d'interès una sèrie de normes tècniques: la família UNE 71505. Sistema de Gestió d'Evidències Electròniques (AENOR, 2013), les ISO IEC 29147:2018 Information technology - Security techniques - Vulnerability disclosure (ISO, 2018) i ISO IEC 29100 Framework sobre protecció de dades d'informació personal (ISO , 2015). És de molt d'interès respecte al tema el Reglament (UE) Núm. 611/2013 relatiu a les mesures aplicables a la notificació de casos de violació de dades personals en el marc de la Directiva 2002/58/CE del Parlament Europeu i del Consell sobre la privacitat i les comunicacions electròniques (Parlamento Europeo, 2013).

Més sobre riscos: d'alt interès relacionar-lo amb la nostra normativa pròpia de seguretat (Reial Decret Llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació) (BOE, 2018), el Reial Decret 704/2011, de 20 de maig, pel qual s'aprova el Reglament de protecció de les infraestructures crítiques (BOE, 2011), la Llei 8/2011, de 28 d'abril, per la qual s'estableixen mesures per a la protecció de les infraestructures crítiques (BOE, 2011), la Directiva (UE) 2016/1148 relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i sistemes d'informació a la Unió (Parlamento Europeo, 2016) i no menys important, la Guia de Seguretat de les TIC CCN-STIC 817: Esquema Nacional de Seguretat. Gestió de Ciberincidents (CCN, 2018).

Sobre el consentiment, és d'alt interès estudiar les directrius sobre el consentiment del Grup 29 (GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS, 2017).

Per a treball amb perfils és molt important la consulta de les directrius sobre decisions individuals automatitzades i elaboració de perfils als efectes del Reglament 2016/679 (Parlamento Europeo, 2018).

Bibliografia

PARLAMENT EUROPEU I CONSELL DE LA UNIÓ EUROPEA. (9 de juliol de 2008). REGLAMENT (CE) Núm.765/2008. - *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, Unió Europea: *Diari Oficial de la Unió Europea*.

AENOR. (Desembre de 2012). *Evaluación de la Conformidad. UNE-EN ISO/IEC 17065*. Madrid, Espanya: AENOR.

AENOR. (2013). *UNE 71505. Sistema de Gestión de Evidencias Electrónicas.* Madrid: AENOR.

AEPD. (2016). *Directrices para la elaboración de contratos entre responsables y encargados de tratamiento.* Madrid: AEPD.

AEPD. (2016). *Guía para el cumplimiento del deber de informar.* Madrid: AEPD.

AEPD. (2017). *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.* Madrid: AEPD.

AEPD. (2017). *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetos al RGPD.* Madrid: AEPD.

AEPD. (2018). *Listado de cumplimento normativo.* Madrid: AEPD.

AEPD, & INCIBE. (2017). *Guía para la gestión y notificación de brechas de seguridad.* Madrid: AEPD.

Agència Catalana de Protecció de Dades. (2018). *Pautes de protecció de dades per als centres educatius.* Barcelona: APDCAT.

Agencia Española de Protección de Datos. (2017). Denúncia de l'AJUNTAMENT DE LA FONT DE LA FIGUERA. *PS/00576/2017*. Madrid, Espanya: Agencia Española de Protección de Datos.

Agencia Española de Protección de Datos. (2017). Google Street View. *Procediment Núm. PS/00541/2010*. Madrid, Espanya: Agencia Española de Protecció de Dades.

Agencia Española de Protección de Datos. (2017). Infracción de Administraciones Públicas instruido por la Agencia Española de Protección de Datos al AYUNTAMIENTO DE BOECILLO. *Procediment Núm. AP/00023/2017*. Madrid, Espanya: Agencia Española de Protección de Datos.

Agencia Española de Protección de Datos. (26 de maig de 2018). *Agencia Española de Protección de Datos.* Recuperat el 18 de juliol de 2018, de https://www.aepd.es/

ARTICLE 29 DATA PROTECTION WORKING PARTY. (27 de febrer de 2013). Opinion 02/2013 on apps on smart devices. Brussel·les, Unió Europea: Consell d'Europa.

Autoritat Catalana de Protecció de Dades. (2018). *Avaluació d'impacte relativa a la protecció de dades.* Barcelona: APDCAT.

Barlow , J. P. (Novembre de 1993). A plain text on crypto policy. *Communications of the ACM, 36*(11), 21-26.

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

BOE. (14 de desembre de 1999). Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal. *BOE núm. 298, de 14/12/1999*. Madrid, Espanya: BOE.

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

BOE. (2011). *Llei 8/2011, de 28 d'abril, per la qual s'estableixen mesures per a la protecció de les infraestructures crítiques.* Madrid: BOE.

BOE. (2011). *Reial Decret 704/2011, de 20 de maig, pel qual s'aprova el Reglament de protecció de les infraestructures crítiques.* Madrid: BOE.

BOE. (5 de desembre de 2018). Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals. *Llei Orgànica 3/2018*. Madrid: BOE.

BOE. (2018). *Reial Decret Llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació.* Madrid: BOE.

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

CCN. (2018). *Guia de Seguretat de les TIC CCN-STIC 817: Esquema Nacional de Seguretat. Gestió de Ciberincidents.* Madrid: CCN.

CNIL. (1 de juny de 2019). *Privacy Impact assessment (PIA)*. Obtingut de https://www.cnil.fr/en/privacy-impact-assessment-pia

Colmenarejo Fernández, R. (2017). *Una ética para Big Data.* Barcelona: UOC.

Comissió Europea. (10 de gener de 2017). 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, Unió Europea: Comissió Europea.

Comissió Europea. (24 de gener de 2018). 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 de 2018. *COMUNICACIÓ DE LA COMISSIÓ AL PARLAMENT EUROPEU I AL CONSELL*. Brussel·les, Unió Europea: Comissió Europea.

Davara Fernández de Marcos, L. (Madrid). *Menores en Internet.* 2017: AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

Davara Rodríguez, M. Á. (1998). *La protección de datos en Europa.* Madrid: Asnef Equifax.

De la Cueva, J. (maig-juny de 2018). Código fuente, algoritmos y fuentes del Derecho. *El Notario del Siglo XXI* (77).

De Miguel Molina, M., & Oltra Gutiérrez, J. V. (2007). *Deontología y Aspectos Legales de la Informática: cuestiones jurídicas, técnicas y éticas básicas.* València: Servei de Publicacions de la Universitat Politècnica de València.

De Miguel Molina, M., Oltra Gutiérrez, J. V., & Sarabdeen, J. (2010). "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)*, 277-285.

Delgado Carravilla, I., & Puyol Montero, J. (2018). *La Implantación del Nuevo Reglamento General de Protección de Datos de la Unión Europea.* València: Tirant.

Dret a l'oblit digital. Digitalització d'hemeroteca sense utilitzar codis ni instruccions que..., STS 4132/2015 - ECLI:ES:TS:2015:4132 (Tribunal Suprem. Sala Civil, 15 d'octubre de 2015).

Diari Oficial de la Unió Europea. (27 d'abril de 2016). *Reglament General de Protecció de Dades (RGPD).* Recuperat el 4 d'abril de 2018, de https://www.boe.es/doue/2016/119/L00001-00088.pdf

Directiva (UE) 2016/680 del Parlament Europeu i del Consell, de 27 d'abril de 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 fins de prevenció. (27 d'abril de 2016). *PARLAMENT EUROPEU I CONSELL DE LA UNIÓ EUROPEA*. Brussel·les, Unió Europea: *Diari Oficial de la Unió Europea*.

Europea, C. d. (19 d'abril de 2018). Errata Reglament General de Protecció de Dades. Brussel·les, UE: Consell de la Unió Europea.

FISCALÍA GENERAL DEL ESTADO. (11 de gener de 2013). SOBRE PAUTAS EN RELACIÓN CON LA DILIGENCIA DE INTERVENCIÓN DE LAS COMUNICACIONES TELEFÓNICAS. *CIRCULAR 1/2013,*. Madrid, Espanya: FISCALÍA GENERAL DEL ESTADO.

Foucalt, M. (2012). *Vigilar y castigar.* Madrid: Biblioteca Nueva.

Frosini, V. (1982). *Cibernética, Derecho y sociedad.* Madrid: Tecnos.

García Mirete, C. M. (2014). *Bases de Datos Electrónicas Internacionales.* València: Tirant lo Blanch.

Garriga Domínguez, A. (2010). *Fundamentos éticos y jurídicos de las TIC.* Cizur Menor (Navarra): Thomson Reuters.

Goizueta Vértiz, J., González Murua, A. R., & Pariente, D. I. (2013). *El espacio de libertad, seguridad y justicia: Schengen y protección de datos.* Cizur Menor (Navarra): Thomson Reuters.

Gómez Sáez , F. (2014). Los reportajes de investigación con cámara oculta y sus repercusiones en los derechos fundamentales. *Tesi Doctoral*. Madrid, Espanya: UNED.

Google Spain SL i Google Inc. contra Agencia Española de Protección de Datos (AEPD) i Mario Costeja González, Assumpte C-131/12 (Tribunal de Justícia de la Unió Europea (Gran Sala) 2014).

Google vs Mario Costeja, C-131/12 (Gran Sala. Tribunal de Justícia - UE 31 de maig de 2014).

GRUP DE TREBALL DE PROTECCIÓ DE LES PERSONES (Grup de treball de l'article 29). (10 d'abril de 2018). Directrius sobre el consentiment en el sentit del Reglament (UE) 2016/679. *17/ES. WP259 i rev.01*. Brussel·les, Unió Europea: Comissió Europea.

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

Grup "Protecció de dades" de l'article 29. (2017). *Directrius sobre l'avaluació d'impacte relativa a la protecció de dades (EIPD) WP 248.* Brussel·les: Comissió Europea.

Grup de treball sobre protecció de dades de l'article 29. (2018). *Directrius sobre la notificació de les violacions de la seguretat de les dades personals d'acord amb el reglament 2016/679.* Brussel·les: UE.

Hobbes, T. (2003). *Leviatan.* Barcelona: Losada.

ISO . (2015). *ISO IEC 29100 Framework sobre protección de datos de información personal.* Madrid: ISO.

ISO. (2018). *ISO IEC 29147:2018 Information technology - Security techniques - Vulnerability disclosure.* Madrid: ISO.

Landau, S., Kent, S., Brooks, C. C., Charney, S., Denning, D. I., Diffie, W., . . . Sobel , D. L. (Agost de 1994). Crypto policy perspectives. *Communications of the ACM, 37*(8), 115-121.

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

Medinacelli Diaz, K. I. (2016). *El tratamiento de los datos sanitarios.* Madrid: Agencia Española de Protección de Datos.

Moore , M. (Direcció). (2007). *Sicko* [Pel·lícula].

Negroponte, N. (2003). Cómo vencer en la revolución digital. Madrid: Conferència ExpoManagement 2003.

Oltra Gutiérrez, J. V. (2001). Echelon hoy. *Novática: Revista de la Asociación de Técnicos de Informática, 153* , 52-55.

Ortega y Gasset, J. (1968). *Meditación de la técnica.* Madrid: *Revista de Occidente*.

Parlament Europeu. (24 de juny de 2013). Reglament (UE) Núm. 611/2013 relatiu a les mesures aplicables a la notificació de casos de violació de dades personals en el marc de la Directiva 2002/58/CE del Parlament Europeu i del Consell sobre la privacitat i les comunicacions electròniques. Brussel·les: UE.

Parlament Europeu. (2016). *DIRECTIVA (UE) 2016/1148 DEL PARLAMENT EUROPEU I DEL CONSELL.* Brussel·les: UE.

Parlament Europeu. (2018). *Directrius sobre decisions individuals automatitzades i elaboració de perfils.* Brussel·les: Parlament Europeu.

PARLAMENT EUROPEU I CONSELL DE LA UNIÓ EUROPEA. (31 de desembre de 2003). 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, Unió Europea: *Diari Oficial de la Unió Europea*.

Real Academia Española. (2017). *Diccionario de la Real Academia Española*. Recuperat el 17 de juliol de 2018, de http://dle.rae.es/

Recurs de cassació per infracció de preceptes constitucionals i infracció de Llei, STS 1942/2016 - ECLI:ES:TS:2016:1942 (Tribunal Suprem. Sala Penal 3 de maig de 2016).

Rincón, R. (26 de juny de 2018). *El País*. Recuperat el 18 de juliol de 2018, d'El Constitucional extiende el derecho al olvido a las hemerotecas digitales: https://elpais.com/politica/2018/06/26/actualitat/1530007122_707929.html

Salvador, P., Rubí, A., & Ramírez, P. (2011). Imágenes veladas. *InDret*.

Secretaria d'Estat de Cultura. (s.f.). *Biblioteca Virtual de Prensa Histórica*. Recuperat el 18 de juliol de 2018, de http://prensahistorica.mcu.es/es/consulta/busqueda.cmd

The International Trade Administration. (27 de juliol de 2016). *EUROPEAN UNION: TRANSFERRING PERSONAL DATA FROM THE EU TO THE US*. Recuperat el 20 de juliol de 2018, de https://www.export.gov/article?id=European-Union-Transferring-Personal-Data-From-the-EU-to-the-US

Vázquez, J. M., & Barroso , P. (1992). *Deontología de la informática. Esquemas.* Madrid: Instituto de Sociología Aplicada.

Warren, S. D., & Brandeis, L. D. (15 de desembre de 1890). The Right to Privacy. (T. H. Association, Ed.) *Harvard Law Review, 4*(5), 193-220.

Contingut