apdcat
Autoritat Catalana de Protecció de Dades

La privacitat des del disseny i la privacitat per defecte

Guia per a desenvolupadors

Febrer 2023

Col·lecció guies. Núm. 7

Generalitat de Catalunya

Índex

1. Introducció

El concepte de la privacitat des del disseny, desenvolupat ja des de finals dels anys 90 en gran mesura gràcies a l'activitat del Comissionat de Protecció de Dades d'Ontàrio, fa referència a la necessitat de tenir en compte l'impacte en termes de privacitat dels productes o serveis, especialment els tecnològics, ja des de la fase del seu disseny.

Estretament lligat amb aquest concepte apareix també el de la privacitat per defecte, que requereix aplicar les mesures tècniques i organitzatives adequades per garantir que, sense que l'usuari hagi de fer cap tipus d'acció (per defecte), únicament es tracten les dades personals indispensables per a cadascuna de les finalitats específiques del tractament.

Amb l'aprovació del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades, d'ara endavant RGPD), tant la protecció de dades des del disseny, com la protecció de dades per defecte passen de ser una recomanació o una bona pràctica a ser una obligació.

En concret, l'article 25 de l'RGPD exigeix:

1. Que, ja des del moment en què es dissenyi un servei o una aplicació, s'implementin les mesures tècniques i organitzatives adequades, com ara la pseudonimització, la minimització de dades i altres garanties per aplicar de manera efectiva els principis de la protecció de dades personals, per garantir el compliment de l'RGPD i els drets i les llibertats de les persones interessades (**protecció de dades des del disseny**).

2. Que s'apliquin les mesures tècniques i organitzatives adequades per garantir que, per defecte, les dades personals que es tractin i l'abast del tractament que se'n faci siguin només els necessaris per a cadascuna de les finalitats específiques del tractament (**protecció de dades per defecte**).

Aquesta obligació s'aplica a:

- La quantitat de dades que es recullen.
- L'abast del tractament.
- El termini de conservació.
- L'accessibilitat de les dades, de manera que, per defecte, les dades no siguin accessibles a un públic indeterminat sense la intervenció de la persona afectada.

Detectar aquestes necessitats i donar-hi solució ja des del mateix moment del disseny de les eines tecnològiques permet estalviar temps, recursos, perjudicis a les persones afectades i els evidents costos reputacionals, que es poden derivar de la incorporació tardana d'aquests requeriments.

Per altra banda, en ser una obligació, incomplir-la pot constituir una infracció de conformitat amb l'RGPD, que pot comportar una sanció de fins a 10.000.000 euros o d'un 2% del volum

de negoci total anual global de l'exercici anterior si el resultat d'aquest càlcul resulta superior als 10.000.000 d'euros.

En qualsevol cas, més enllà d'aquesta obligació, la protecció de dades constitueix cada vegada més un factor qualitatiu valorat per les empreses i les institucions que adquireixen un determinat producte o servei i també per les persones usuàries.

En definitiva, la protecció de dades és un avantatge competitiu i aquesta guia pretén ser un mitjà útil per poder treure'n profit.

Des de l'Autoritat Catalana de Protecció de Dades (APDCAT) considerem estratègicament prioritari que els diferents actors de l'ecosistema digital ho percebin així. Per això, aquesta guia s'elabora per facilitar als desenvolupadors, i també als responsables del tractament que els encarreguen el desenvolupament d'aplicacions, la identificació dels diferents elements rellevants per a la protecció de les dades personals, i les mesures que es poden adoptar per fer-hi front, ja des del moment del disseny.

2. Els rols vinculats a la protecció de dades des del disseny i per defecte

La protecció de dades des del disseny i per defecte, tal com preveu l'RGPD, té com a destinatari directe el responsable del tractament, que és qui té l'obligació d'aplicar i vetllar perquè s'apliquin les mesures tècniques i organitzatives que corresponguin.

Per identificar qui és el responsable del tractament cal tenir en compte la definició de l'apartat 7 de l'article 4 de l'RGPD, que defineix el responsable com qui determina les finalitats del tractament de dades i els mitjans que s'empraran.

En tot cas, el mateix RGPD preveu la possibilitat que el responsable delegui el tractament de les dades en un tercer o, simplement, li permeti accedir a les dades per prestar un servei per compte del responsable. És el que s'anomena "encarregat del tractament". Aquesta figura pot abastar tant les entitats prestadores del servei en si mateix (com ara un concessionari d'un servei públic), com els que col·laboren amb el responsable per prestar-lo (per exemple, un servei d'allotjament (*hosting*) o una empresa que faci el desenvolupament o el manteniment d'una aplicació o plataforma que comporti accedir o tractar dades personals). En qualsevol cas, si el desenvolupador necessita accedir a dades personals per compte del responsable del tractament, encara que només sigui en la fase de desenvolupament, cal formalitzar un contracte amb el contingut que preveu la normativa de protecció de dades[1].

Cal destacar que el responsable ha d'escollir un encarregat del tractament que ofereixi prou garanties pel que fa a l'aplicació de mesures tècniques i organitzatives apropiades. Així, un element a tenir en compte a l'hora de fer aquesta elecció és que l'encarregat disposi de segells o certificacions o de procediments i protocols d'actuació que incorporin la protecció de dades des del disseny i per defecte.

[1] Vegeu article 28 de l'RGPD.

Especialment, cal tenir en compte que les dades personals només es poden transferir fora de l'espai econòmic europeu si el país de destí té una decisió d'adequació dictada per la Comissió Europea,[2] o es tenen garanties adequades d'acord amb algun dels mecanismes previstos a l'article 46 de l'RGPD.

En qualsevol cas, les mesures que el responsable ha de complir en virtut dels articles 25 i 32 de l'RGPD també les ha d'imposar a l'encarregat del tractament i, així mateix, les ha d'exigir als productes i serveis que adquireixin o que encarreguin.

En altres termes, els nous productes i serveis desenvolupats, ja siguin interns (del mateix responsable o encarregat del tractament) o externs, han de complir amb la protecció de dades des del disseny i per defecte. Altrament, el responsable del tractament no podrà complir les seves obligacions.

Per altra banda, no és descartable que els desenvolupadors que tinguin la consideració d'encarregats del tractament subcontractin alguna actuació a tercers (allotjament, utilització d'eines facilitades per tercers, etc.) que comporti que hagin d'accedir a dades personals. Aquests tercers reben la consideració de subencarregats. En aquest cas, el desenvolupador que tingui la consideració d'encarregat del tractament ha d'escollir un sostencarregat que ofereixi garanties adequades i ha de disposar de l'autorització del responsable. Al sostencarregat li són aplicables les mateixes obligacions i garanties que a l'encarregat del tractament.

A títol de resum, en el desenvolupament d'una solució tecnològica encarregada a un tercer que, a la vegada, encarrega a un altre tercer l'allotjament durant aquesta fase, els principals rols es recullen a la taula que figura a continuació:

Rols	**Responsable**	**Encarregat**	**Subencarregat**
Funció	Determina les finalitats i els mitjans del tractament de dades personals	Presta un servei al responsable que implica accedir a dades personals	Presta un servei a l'encarregat que implica accedir a dades personals
Exemple	Entitat que inicia una solució tecnològica que implica tractar dades personals	Desenvolupadors	Servei d'allotjament (hosting)

Cal remarcar que, perquè la protecció de dades des del disseny i per defecte sigui efectiva, s'ha de garantir especialment que els desenvolupadors han tingut en compte el context en el qual s'acabarà aplicant el seu desenvolupament. Per configurar el producte amb totes les

[2] La llista de països amb una decisió d'adequació es pot consultar en aquest enllaç.

garanties adequades, és indispensable conèixer les circumstàncies en les quals s'executarà l'aplicació.

Aquest coneixement i la implementació de les garanties corresponents constitueix un clar avantatge competitiu, ja que el responsable del tractament ha de prioritzar les solucions més adients per garantir els drets de les persones usuàries.

3. L'aplicació efectiva de la protecció de dades des del disseny i per defecte

La normativa que regula la protecció de dades des del disseny i per defecte no determina quines mesures tècniques i organitzatives concretes cal implementar. La determinació de les mesures necessàries ha de ser el resultat d'una anàlisi prèvia feta pel responsable del tractament i, per extensió, pels desenvolupadors de les solucions tecnològiques que ha d'emprar el responsable del tractament.

Cal aplicar les mesures que siguin necessàries i proporcionades. En qualsevol cas, en el moment del disseny cal tenir en compte:

- La naturalesa, l'àmbit, el context i les finalitats del tractament.
- Els riscos que comporta el tractament per als drets i les llibertats de les persones.
- L'estat de la tècnica.
- El cost de l'aplicació.

En principi, la definició de la naturalesa, l'àmbit, el context i les finalitats del tractament correspon al responsable del tractament. L'elecció d'una determinada solució tecnològica ha de tenir en compte aquests elements, però també els riscos inherents a cada tecnologia disponible. Per això, la col·laboració dels desenvolupadors esdevé essencial ja en aquesta fase.

Un cop coneguts aquests aspectes, cal valorar els riscos que comporta el tractament per als drets i llibertats de les persones. Si es preveu que poden ser alts, cal fer una avaluació d'impacte de protecció de dades (AIPD).[3] En aquesta valoració ja és rellevant que hi participi el desenvolupador, atès que probablement és qui està en una posició millor per avaluar les tecnologies que es poden emprar i que poden implicar un risc elevat per als drets i llibertats de les persones que faci necessària l'AIPD.[4] També, per contribuir a definir quines mesures es poden implementar per reduir aquest risc, tenint en compte l'estat de la tècnica i el cost d'aplicació. En resum, l'avaluació d'impacte sobre la protecció de dades és un procés sistemàtic que, a banda de requerir una descripció sistemàtica del tractament previst i de la seva necessitat i proporcionalitat, requereix (i) avaluar els riscos derivats del tractament i (ii) determinar les mesures per mitigar aquests riscos.[5]

[3] L'article 35 de l'RGPD conté una llista de supòsits no exhaustiva. També és d'utilitat la relació continguda a l'article 28.2 de la LO 3/2018 i la llista publicada per l'APDCAT.
[4] L'APDCAT disposa de materials i fins i tot d'una aplicació per poder fer aquesta avaluació d'impacte de protecció de dades.
[5] Si els riscos no es poden mitigar prou, abans d'iniciar el tractament cal consultar l'autoritat de control.

Igualment, en els casos en què no sigui exigible fer una AIPD, cal que es valorin les opcions tècniques disponibles tenint en compte l'estat actual de la tècnica, així com el cost d'implementar-les.

Amb aquesta finalitat, seran d'utilitat les tecnologies que milloren la protecció de la privacitat (*privacy enhancing technologies* o *PET*), que permeten minimitzar els riscos sense perdre la funcionalitat de l'aplicació o el sistema d'informació. A l'apartat 4 d'aquesta guia es recullen algunes mesures que es consideren clau per a la protecció de les dades personals i que formen part d'aquest conjunt més general conegut com a PET.

En definitiva, el disseny de solucions tecnològiques ha de tenir en compte els riscos derivats del tractament per determinar les mesures tècniques que cal aplicar.

La protecció de dades en el disseny i la protecció de dades per defecte s'han de projectar en les diferents fases del tractament de les dades:

- Disseny.
- Desenvolupament i proves.
- Recollida de les dades.
- Ús de les dades.
- Comunicació o divulgació de les dades.
- Manteniment i conservació de les dades.

A continuació, s'identifiquen sense cap ànim d'exhaustivitat alguns dels aspectes que es considera clau de valorar en relació amb cadascuna d'aquestes fases i que, des del mateix moment del disseny, han de fer possible el compliment dels principis de protecció de dades personals.

A fi de facilitar la revisió sistemàtica dels elements que se suggereix valorar en relació amb les diferents fases que conformen el tractament de dades personals, s'ha confeccionat un llistat específic (*checklist*) que figura com a annex d'aquesta guia. A manera de resum, aquesta llista recull els principals aspectes a tenir en compte, que es comenten més detalladament als apartats 3 i 4 d'aquesta guia i permetrà avaluar el grau d'incorporació de la protecció de dades en el disseny de les solucions.

3.1 Fase de disseny

En la fase de disseny de les solucions tecnològiques es defineixen els diferents components en què s'estructurarà el programari i les seves interaccions, amb l'objectiu de complir una sèrie de requeriments funcionals i no funcionals. La protecció de dades des del disseny i per defecte introdueix la protecció de dades entre aquests requeriments.

La complexitat inherent al desenvolupament de programari fa que l'ús d'una metodologia de desenvolupament sigui essencial per gestionar els projectes i aconseguir que siguin exitosos.

Si bé la protecció de dades des del disseny i per defecte no implica l'ús de noves metodologies de disseny, sí que requereix ajustar les tasques o les anàlisis que es duen a terme. En aquest sentit, es parla de diferents estratègies de disseny:[6]

- **Minimitzar**: limitar al mínim possible el tractament de dades personals. Tractar les mínimes dades personals, limita l'impacte que el sistema pugui tenir sobre les persones.

- **Amagar**: amagar les dades personals de qui no cal que les conegui, cosa que dificulta que se'n pugui fer un mal ús. Hi ha múltiples maneres d'amagar-les, i la seva utilitat depèn de la situació concreta: criptografia, control d'accés, etc.

- **Separar:** tractar les dades de manera distribuïda i en compartiments al més separats possible. Separar les dades en diferents compartiments estancs evita que es pugui accedir fàcilment als perfils complets de les persones.

- **Agregar:** tractar les dades de la manera més agregada possible, sempre que permeti assolir la finalitat perseguida. L'agregació de dades en grups de persones, si són prou grans i diversos, fa que les dades no es puguin associar a una persona concreta.

- **Informar:** informar adequadament les persones sobre el tractament de les seves dades personals.

- **Controlar:** les persones han de poder decidir sobre el tractament de les seves dades.

- **Fer complir:** hi ha d'haver una política de privacitat, compatible amb els requeriments legals, i s'han de posar els mitjans perquè es compleixi.

- **Demostrar:** Cal ser capaç d'evidenciar que el tractament de dades personals es dur a terme de manera "amigable" en termes de privacitat.

A nivell més pràctic hi ha els patrons de privadesa, que donen solucions de disseny a problemes comuns en protecció de dades.[7] És a dir, són una forma ja validada d'aplicar les estratègies de disseny a problemes concrets.

Durant el disseny d'una solució, cal incloure com a elements essencials la determinació dels fluxos de la informació personal que es tractarà (d'on es recullen les dades, com es recullen, qui ha de tenir-hi accés i per a què, etc.) i les mesures de seguretat exigibles en cada supòsit concret.

Aquestes mesures dependran del resultat de l'anàlisi de riscos que cal fer en tots els casos. En els apartats següents d'aquesta guia s'analitzen moltes d'aquestes mesures, agrupades

[6] Privacy Design Strategies (The Little Blue Book), JAAP-HENK HOEPMAN (2022)
[7] Patrons de privadesa.

d'acord amb la fase del tractament en què tenen més rellevància. Però és en el moment del desenvolupament de l'aplicació que cal tenir-les en compte per incorporar-les en el disseny.

3.2 Fase de desenvolupament i de proves

La majoria de les vegades, el desenvolupament de programari i les proves exigeixen l'ús de dades. Quan aquestes dades són personals, la normativa de protecció de dades és de plena aplicació.

Aspectes a tenir en compte pel que fa a la utilització de dades durant les fases de disseny i de proves

- Si en la fase de desenvolupament i de proves cal tenir accés a dades personals, l'equip o l'empresa de desenvolupament i les que contracti el desenvolupador seran encarregats del tractament (vegeu l'apartat 2 d'aquesta guia sobre "Els rols vinculats a la protecció de dades des del disseny i per defecte").

- Per garantir la confidencialitat i la integritat de la informació cal separar adequadament l'entorn de producció i el de desenvolupament i proves i garantir que l'entorn de proves és segur (si és possible, aïllat de connexions externes fins al moment que resulti imprescindible).

- Si es poden fer desenvolupaments i proves sense necessitat d'emprar dades reals, cal optar per aquesta possibilitat. En general, és possible utilitzar dades sintètiques (vegeu l'apartat 4 d'aquesta guia).

  Si no es pot, cal utilitzar les dades mínimes. Pel terme minimitzar no ens referim només a la quantitat, sinó també a la qualitat (presència d'identificadors i pseudoidentificadors, nivell de detall, etc.).

  En el cas que convingui emprar dades reals, si és possible utilitzar-les anonimitzades o pseudonimitzades es recomana decantar-se per alguna d'aquestes opcions.

  Si cal emprar dades, es poden reutilitzar dades de les quals ja disposava el responsable o recollir-les de nou. En aquest darrer cas, cal tenir en compte les recomanacions que es fan a l'apartat 3.3 d'aquesta guia.

- Cal prestar especial atenció a la ubicació del servidor on s'allotjarà la informació recollida. Aquesta circumstància pot arribar a comprometre la confidencialitat de la informació, atès que no tots els països apliquen les mateixes garanties. A més, emprar un servidor de fora de l'espai econòmic europeu implica que es produeixi una transferència internacional de dades que perquè sigui vàlida ha de complir determinats requisits (capítol V de l'RGPD).

- S'han d'implementar mecanismes de control d'accés per evitar que usuaris no autoritzats accedeixin a les dades. Cal crear un usuari per a cada persona que hagi d'accedir-hi i limitar l'accés a les dades necessàries per desenvolupar les seves funcions.
- Les còpies de seguretat de la infraestructura de desenvolupament i prova són essencials per a l'èxit del projecte, però cal tenir en compte que si aquestes còpies contenen dades personals cal controlar-hi l'accés.
- Quan s'emprin xarxes wifi, cal utilitzar el protocol que proporcioni el grau de seguretat més alt[8].
- El paquets de programari i llibreries que s'utilitzin en el desenvolupament han d'estar actualitzats. La manca d'actualització pot donar lloc a vulnerabilitats en el programari desenvolupat.
- L'entitat desenvolupadora ha de formar el seu personal en matèria de protecció de dades i ha d'establir els compromisos de confidencialitat escaients.

Altres aspectes a tenir en compte en la fase de disseny

- Utilitzar alguna metodologia per garantir la qualitat del codi font. Bé sigui manual, mitjançant revisions del codi fetes per diferents persones, o automàtica amb eines d'anàlisi estàtica o dinàmica. Un codi de mala qualitat pot donar lloc a vulnerabilitats, que poden posar en risc les dades personals.
- Seguir les recomanacions de les guies de programació segura.

En la fase de posada en marxa de la solució tecnològica, i també en el moment de la incorporació a l'organització de noves persones usuàries, resulta essencial una formació del personal que l'hagi d'utilitzar, adequada als diversos perfils. Això implica preveure sessions formatives per conèixer el funcionament de la solució, els riscos derivats de fer-ne ús, les mesures organitzatives i tècniques que cal adoptar per minimitzar-los i, també, disposar de manuals d'ús exhaustius.

[8] En aquest sentit, cal tenir present que s'han detectat vulnerabilitats importants dels protocols WEP, WPA i WPA2. En el moment d'elaborar aquesta guia el protocol més recent és el WPA3. També cal tenir en compte que alguns routers més antics podrien no suportar-lo.

3.3 Recollida de les dades

3.3.1 Minimització de les dades

Només s'han de recollir les dades adequades i necessàries per assolir la finalitat perseguida.

D'entrada, això implica que cal plantejar-se si la finalitat es pot assolir sense emprar dades personals. Això simplificaria les obligacions del responsable, atès que la normativa de protecció de dades personals no seria d'aplicació.

Si cal utilitzar dades personals, únicament es poden recollir les mínimes necessàries per assolir la finalitat concreta establerta pel responsable del tractament i de la qual s'ha informat les persones afectades. Encara cal ser molt més restrictiu quan es recullen categories especials de dades (dades que revelen l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques o l'afiliació sindical, dades genètiques, dades biomètriques destinades a identificar de manera unívoca una persona física, dades relatives a la salut o dades relatives a la vida sexual o l'orientació sexual), de manera que, sempre que es pugui, cal evitar recollir aquest tipus de dades.

Les dades que es recullen poden ser molt variades. Poden comprendre, entre altres, les següents:

- Dades identificatives, de contacte, laborals, de formació, socioeconòmiques, sobre aficions, estils de vida, etc., a banda de les categories especials de dades ja esmentades.
- Registres d'activitat, que s'utilitzen en tot tipus de serveis (servidors web, servidors de correu, en una botiga en línia, etc.).
- Dades de geolocalització.
- Dades procedents de dispositius connectats (*wearables*), com ara, pulsacions, pressió arterial, nivell d'oxigen a la sang, etc.) que es recullen automàticament.
- Transaccions (pagaments amb mòbil, amb targeta, etc.).
- Dades identificatives associades a dispositius o protocols de comunicació (adreça IP, adreça MAC, número de telèfon, IMEI, ICC SIM, etc.).
- Metadades associades a fitxers.

Atès que la majoria de productes o serveis digitals recopilen dades constantment, la verificació de la necessitat d'obtenir dades personals s'ha de fer permanentment. Tot i això, el primer accés (caracteritzat sovint per la configuració d'un formulari o la necessitat de donar accés a un perfil prèviament configurat) és un moment especialment sensible en aquest sentit.

La verificació de la necessitat de les dades personals ha de comprendre "totes" les que s'obtinguin, independentment del canal a través del qual s'obtenen. En aquest sentit, cal prestar especial atenció a les dades obtingudes per múltiples fonts – més enllà dels formularis-, entre les quals la recollida de dades sobre l'activitat dels usuaris o les galetes

(*cookies*), ja siguin pròpies o de tercers, que, a més, poden respondre a finalitats diverses (patrons de comportament, dades demogràfiques dels usuaris, etc.).

La recollida es pot produir de manera directa o indirecta. Així, per exemple, quan un desenvolupador utilitza determinades llibreries de tercers, això pot comportar el tractament d'informació personal, fins i tot de vegades de manera inadvertida. Per exemple, en incloure una llibreria Javascript en un web, estem donant accés a aquesta llibreria a la informació personal continguda al web. Encara és més preocupant que les llibreries de tercers utilitzades en el desenvolupament d'aplicacions mòbils tinguin els mateixos permisos que l'aplicació desenvolupada. Això implicaria, per exemple, que si l'aplicació pot accedir a la geolocalització o al micròfon, també ho podrien fer les llibreries externes utilitzades.

Per altra banda, quan una aplicació sol·licita permisos per accedir i recollir informació irrellevant per a la finalitat que persegueix, no s'està complint adequadament el principi de minimització de dades. Per exemple, si es recull informació sobre la geolocalització, quan el servei que s'ofereix és exactament el mateix independentment de la ubicació.

També és important tenir en compte que algun mètode de recollida pot implicar, fins i tot, una transferència internacional de dades fora de l'espai econòmic europeu, cosa que requereix tenir amb garanties adequades d'acord amb l'RGPD. A títol d'exemple, pot succeir que un servei d'obtenció de dades estadístiques dels visitants d'un web remeti automàticament la informació a servidors ubicats fora de l'espai econòmic europeu, de manera que caldrà analitzar si en el país de destinació de les dades hi ha garanties equivalents a les que hi hauria dins l'àmbit europeu.[9]

Aspectes rellevants

- Cal plantejar-se si es pot assolir igualment la finalitat perseguida sense recollir dades personals, o bé recollint-ne menys de les inicialment previstes. És a dir, si hi ha alguna alternativa que permeti aconseguir la finalitat amb menys dades. Una possibilitat podria ser generar dades artificials, que simplement repliquin els comportaments de les dades reals, i treballar exclusivament amb aquestes dades, anomenades sintètiques. També es podria optar per modificar les dades de manera que no es puguin associar a una persona (pseudonimització, anonimització), reduir la quantitat de dades recollides o el nivell de detall, restringir al màxim l'accés a les dades a les parts del sistema que les necessiten, etc.

- Convé evitar de tractar dades de categoria especial si no és estrictament necessari. Per exemple, en lloc de configurar l'accés a un determinat servei digital amb dades biomètriques, es pot fer

[9] En concret, en relació amb l'ús de la solució "Google Analytics", l'Autoritat de Protecció de Dades Francesa – CNIL – al febrer de 2022 va ordenar a una web deixar de fer ús d'aquest servei i va fer públiques unes informacions generals en relació a la utilització de Google analytics. Ja a principis d'any, es va pronunciar en aquesta mateixa línia l'Autoritat de Protecció de Dades Austríaca.

mitjançant una contrasenya i, eventualment, implementar un doble factor d'autenticació.[10]

- Cal ser especialment curosos a l'hora de dissenyar els formularis i, en particular, a l'hora de definir-ne els camps obligatoris. Cal distingir clarament la informació que s'ha de proporcionar obligatòriament de la que és opcional.

- L'aplicació ha de demanar només els permisos per accedir i recollir informació rellevant per a la finalitat que persegueix.

- Cal evitar emmagatzemar per defecte dades tècniques que no siguin estrictament necessàries, com ara l'adreça MAC, l'adreça IP, el nom del dispositiu o l'ID de publicitat.

- Cal evitar obtenir informacions connexes innecessàries (com ara metadades, dades vinculades a l'activitat, etc.).

- Cal valorar la possibilitat que determinada informació es pugui tractar en el mateix dispositiu de la persona usuària. Un exemple clar d'aquesta manera de procedir és el sistema de rastreig descentralitzat per a contactes de risc, durant la pandèmia de COVID-19.

- Cal valorar la possibilitat d'**anonimitzar o pseudonomitzar** les dades, quan no sigui indispensable conèixer la identitat de la persona usuària que hi està vinculada.

- Cal ser curós amb l'ús de components de programari externs, ja que podrien tenir accés a dades personals fins i tot sense que aquest accés estigui documentat. Convé revisar les condicions d'ús d'aquests components i, fins i tot, monitoritzar l'accés a dades personals que fan.

3.3.2 Licitud de la recollida i el tractament de dades

Per poder recollir i tractar informació personal, cal que hi concorri una base jurídica de les que preveu l'article 6 de l'RGPD.

A més, si es tracta de dades de categoria especial (que revelen l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques o l'afiliació sindical; dades genètiques; dades biomètriques destinades a identificar de manera unívoca una persona física; dades relatives a la salut o a la vida sexual o l'orientació sexual), cal que hi concorri alguna de les excepcions que preveu l'article 9.2 de l'RGPD.

[10] Cal recordar en aquest sentit que un doble factor d'autenticació implica la combinació de dos mitjans de verificació consistents en: una informació coneguda per l'usuari – per exemple contrasenya -, quelcom que té – per exemple, el seu telèfon mòbil i quelcom que s'és – per exemple alguna dada biomètrica-.

El consentiment de la persona afectada és una de les bases jurídiques previstes a l'article 6 de l'RGPD i, sovint, es pot emprar com a base jurídica per recollir dades a través d'aplicacions o serveis web que les persones usuàries es poden instal·lar, o a les quals poden accedir de manera voluntària i lliure. El consentiment ha de ser inequívoc, específic, informat i lliure, de manera que la decisió de no prestar-lo no pot tenir altres conseqüències més enllà de les estrictament vinculades a la impossibilitat que es tracti aquella informació.

Aspectes a tenir en compte pel que fa a la gestió del consentiment en el disseny de solucions tecnològiques

- El consentiment ha de consistir en una declaració o acció afirmativa clara i ha de requerir una acció de la persona usuària**.** Pot consistir, per exemple, en una casella que ha d'emplenar, la signatura electrònica o una acció que permeti entendre inequívocament que es consent (per exemple, si s'accedeix a un enllaç després d'haver-ne estat informat de manera clara). No pot ser una opció premarcada.

- Quan el consentiment s'atorga per tractar categories especials de dades, o per rebre comunicacions comercials, cal que sigui explícit. En aquest cas, no n'hi ha prou de poder deduir el consentiment de l'activitat de la persona usuària (per exemple, continuar navegant o accedir a determinats apartats), sinó que cal una declaració expressa.

- El consentiment ha de de ser específic. Quan es demana per a diverses finalitats, la persona usuària ha de poder escollir separadament respecte de cadascuna (consentiment granular), per exemple amb caselles o botons d'opció.

- Abans de demanar el consentiment, cal informar les persones afectades dels aspectes als quals es refereix l'apartat "Transparència i lleialtat per a la persona usuària" d'aquesta guia.

- El consentiment ha de ser lliure. No n'hi ha prou de configurar consentiments diferents per a diferents usos, si s'estableix de manera que per poder seleccionar una determinada opció cal atorgar també el consentiment en un altre àmbit, o es condiciona l'oferiment del servei a consentir per a una altra finalitat que no hi ha d'anar necessàriament lligada.

- Cal conservar els logs o mitjans per acreditar la prestació del consentiment durant tot el tractament de les dades, i fins que no hagi transcorregut el termini de prescripció de les eventuals infraccions derivades del tractament (les infraccions molt greus no prescriuen fins al cap de tres anys que s'hagin produït).

- El consentiment s'ha de poder revocar en qualsevol moment. Cal preveure mecanismes de revocació, separadament per a cadascuna de les finalitats previstes, que siguin accessibles de manera similar a l'obtenció del consentiment.

- Cal establir mecanismes segurs per identificar les persones que presten el consentiment i el revoquen.

- El consentiment atorgat per menors d'edat únicament és vàlid si són més grans de 14 anys.[11] En aquest cas, encara que tinguin una eficàcia limitada, podria ser útil instaurar galetes de sessió que continguin l'edat inicialment introduïda pel menor de tal manera que quan un menor de 14 anys hagi introduït, per exemple, la seva data de naixement i constati que no pot accedir al servei, no li resulti especialment senzill canviar l'edat.

3.3.3 Transparència i lleialtat per a la persona usuària

Per complir els principis de transparència i lleialtat cal garantir que l'usuari pugui conèixer tota la informació necessària sobre com es tracten les seves dades, perquè pugui prendre les decisions que li corresponen o exercir els seus drets, i que el tractament s'adeqüi a les expectatives que la persona afectada s'ha pogut generar a partir d'aquesta informació.

Correspon al responsable del tractament determinar el contingut de les clàusules informatives. No obstant això, en el moment de dissenyar l'aplicació convé tenir en compte determinats aspectes sobre la manera com es facilita aquesta informació.

A més, els principis de transparència i lleialtat també impliquen l'obligació d'abstenir-se d'incórrer en pràctiques conegudes com a patrons foscos (*dark patterns*) o dissenys enganyosos. Aquests patrons són interfícies i implantacions d'experiències que indueixen els usuaris a prendre decisions no intencionades, no desitjades i potencialment perjudicials en relació amb el tractament de les seves dades personals.[12]

El Comitè Europeu de Protecció de Dades recull diverses categories de patrons foscos:

- **Sobrecarregar (*overloading*)**: oferir un excés de peticions, informacions o opcions, per aconseguir que l'usuari comparteixi més dades o involuntàriament permeti que es tractin les seves dades personal en contra de la seva vertadera voluntat. Els següents tres patrons foscos formen part d'aquesta categoria: **indicacions**

[11] Llevat que la normativa aplicable al sector de què es tracti estableixi una altra edat mínima.

[12] EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them. Version 1.0. Adopted on 14th March 2022.
Sobre això, vegeu també les aportacions de Harry Brignull a https://www.deceptive.design/, on es descriuen diverses tipologies de dissenys enganyosos

contínues (c*ontinuous prompting*), **laberint de privacitat** (*privacy maze*), **massa opcions** (*Too Many Options*).

- **Despistar** (*Skipping*): dissenyar la interfície d'experiència d'usuari de manera que els usuaris s'oblidin o no reflexionin sobre els aspectes vinculats a la protecció de dades. Els següents dos patrons foscos formen part d'aquesta categoria: **acolliment enganyós** (*deceptive snugness*) i **mira cap allà** (*look over there*).

- **Manipular** (*Stirring*): la capacitat d'elecció dels usuaris es veu afectada, perquè s'incideix sobre les seves emocions o estímuls visuals. Els següents dos patrons foscos formen part d'aquesta categoria: **conducció emocional** (*emotional steering*) i **oculta a simple vista** (*hidden in plain sight*).

- **Obstaculitzar** (*hindering*): obstaculitzar o bloquejar els usuaris en el seu procés d'obtenció d'informació o gestió de les seves dades, de manera que aquesta tasca esdevingui especialment dificultosa o impossible d'assolir. Els següents tres patrons foscos formen part d'aquesta categoria: **carreró sense sortida** (*dead end*), **més llarg del necessari** (*longer than necessary*) i **informació enganyosa** (*misleading information*).

- **Dissenyar de manera inconsistent** (*fickle*): dissenyar la interfície de manera que sigui inconsistent i poc clara. Com a conseqüència, per a l'usuari és complicat de navegar entre les diferents eines de control de la protecció de dades i entendre la finalitat del tractament. Els següents dos patrons foscos formen part d'aquesta categoria: **absència de jerarquia** (*lacking hierarchy*) i **descontextualització** (*decontextualising*).

- **Ocultar** (*left in the dark*): implica que la interfície es dissenya per ocultar informació o instruments de control de la protecció de dades, o bé per deixar l'usuari sense saber com es tracten les seves dades i com pot controlar-les a través de l'exercici dels seus drets. Els següents tres patrons foscos formen part d'aquesta categoria: **discontinuïtat de llenguatge** (*language discontinuity*), **informació contradictòria** (*conflicting information*) i **redacció o terminologia ambigua** (*ambiguous wording or information*).

Aspectes rellevants

- La informació s'ha de facilitar abans de recollir les dades i, si escau, abans de donar el consentiment.

- Quan les dades no s'obtenen de la persona interessada, també cal informar-la. Cal fer-ho en el termini d'un mes des que s'obtenen o, si es preveu emprar-les en una comunicació, com a màxim en el

moment de la primera comunicació a la persona interessada o a un tercer.

- Cal que la informació sigui completa, simple, entenedora, visualment clara i adaptada, si escau, a les persones amb dificultats funcionals.[13]
- En el cas de serveis adreçats a menors, la informació s'ha de facilitar en un llenguatge adaptat als coneixements d'aquest col·lectiu.
- Quan les dades es recullen de la persona interessada, cal informar-la sobre els aspectes previstos als apartats 1 i 2 de l'article 13 de l'RGPD. Si qui facilita les dades és una tercera persona, cal donar la informació que preveuen els apartats 1 i 2 de l'article 14 de l'RGPD.
- La informació es pot facilitar per capes. Així, d'entrada s'informa sobre la finalitat del tractament, la identitat del responsable i la possibilitat d'exercir els drets de l'autodeterminació informativa (dret d'accés, rectificació, supressió, oposició, limitació del tractament i portabilitat) i qualsevol altra informació que es considera indispensable i, a més, s'ofereix a la persona usuària la possibilitat de consultar la resta de la informació, si vol conèixer més detalls sobre les implicacions del servei.
- La informació que es proporciona ha de ser fidedigna. Qualsevol modificació s'ha de comunicar a la persona usuària clarament i amb celeritat perquè pugui prendre les decisions oportunes.
- Cal preveure que s'efectuïn còpies dels webs i les aplicacions, per poder verificar els mecanismes i el contingut de les clàusules informatives existents en cada moment aplicant un segell de temps verificable (*timestamp*).
- Cal abstenir-se d'implementar patrons foscos.

3.4 Ús de les dades

Les dades personals que es recullen no es poden utilitzar per a qualsevol finalitat. La finalitat ha de ser determinada (no pot ser confusa o massa genèrica), explícita (ha d'estar recollida a la informació facilitada a la persona afectada i al Registre d'activitats del tractament que ha de portar el responsable del tractament) i legítima (vegeu l'apartat "*Licitud de la recollida i el tractament de dades"* d'aquesta guia).

[13] Cal tenir en compte la normativa sobre accessibilitat: Directiva 2016/2102 del Parlament Europeu i del Consell, de 26 d'octubre de 2016, sobre l'accessibilitat dels llocs web i aplicacions per a dispositius mòbils dels organismes del sector públic; Reial decret 1112/2018, de 7 de setembre, sobre accessibilitat dels llocs web i aplicacions per a dispositius mòbils del sector públic. També pot ser d'interès: Accessibility requirements for ICT products and services i Web Content Accessibility Guidelines.

L'ús efectiu que se'n faci ha de correspondre sempre a la finalitat respecte de la qual es va informar la persona afectada, en recollir les dades. Només es poden emprar per a altres finalitats si es té el consentiment de la persona afectada, si una llei ho autoritza o si es tracta d'una activitat que es pugui considerar compatible, d'acord amb els criteris que estableix l'RGPD.[14]

Aspectes rellevants

- Convé instaurar mecanisme tècnics d'autocontrol que garanteixin que l'ús de la informació queda en tot moment circumscrit a la finalitat declarada. Cal disposar d'un sistema adequat de classificació de la informació, que garanteixi que l'ús que se'n fa queda delimitat a l'ús legítim que se'n pot fer.

- Cal instaurar mecanismes adequats de protecció per evitar l'ús indegut per part d'agents externs a l'organització –per exemple encarregats del tractament- o interns (cal tenir present que sovint el risc més significatiu prové del personal de la mateixa organització). Sobre aquesta qüestió ens remetem a l'apartat sobre la confidencialitat d'aquesta guia.

- Es recomana dissenyar les solucions tecnològiques de manera que es faciliti l'exercici dels drets de les persones afectades (dret d'accés, rectificació, supressió, oposició, limitació del tractament i portabilitat), si és possible a través de la mateixa aplicació, i que també facilitin que el responsable els pugui fer efectius fàcilment.

3.5 Comunicació o divulgació de les dades

Cal assegurar que només es produeixen comunicacions de dades a terceres persones quan hi ha una base jurídica per fer-ho i s'han adoptat les mesures de seguretat adequades.

Aspectes rellevants

- Quan la utilització d'una aplicació o d'una solució tecnològica es basa en el consentiment de la persona afectada, cal establir mecanismes perquè, per defecte, les dades no siguin accessibles a un nombre indeterminat de persones sense la intervenció de la persona afectada.

[14] Articles 5.1.*b* i 6.4 de l'RGPD.

- Quan a través de la solució tecnològica es publica informació, convé preveure mecanismes que en possibilitin la despublicació automatitzada, un cop transcorri el termini de publicació establert.

- Es recomana que les comunicacions es facin amb **xifratge d'extrem a extrem.** Això permet que les dades únicament puguin ser desxifrades en el dispositiu del receptor de les comunicacions -mitjançant la seva clau privada- i no per exemple pels proveïdors del servei de comunicacions.

En serveis web, cal emprar el **protocol HTTPS** i configurar el servidor de manera que no sigui possible accedir-hi a través d'altres protocols. Aquest protocol de comunicació, basat en l'ús de certificats per part del servidor, és particularment interessant ja que no només garanteix la confidencialitat i la integritat (xifratge), sinó també l'autenticitat del prestador de serveis. Això es pot complementar amb el protocol HSTS, que instrueix el navegador per utilitzar només HTTPS; així s'evita el risc d'atacs MitM, especialment si es fa una precàrrega de la capçalera HSTS.

- Cal analitzar si el destinatari de les dades necessita accedir-hi en clar. Si no és així (com ara un encarregat del tractament que només ha d'allotjar la informació), cal xifrar les dades de manera que no hi pugui accedir.

- Si el destinatari necessita accedir-hi per fer operacions de càlcul, cal avaluar la possibilitat que tingui accés només a dades amb xifratge homomòrfic. Hi ha situacions en què això és particularment interessant, com ara quan es vol utilitzar el núvol per emmagatzemar dades i fer càlculs.

En la mateixa línia, cal tenir en compte que hi ha una gran quantitat de protocols criptogràfics que permeten fer una varietat de tasques revelant la informació mínima. Per exemple, esquemes de compartició de secrets, proves de coneixement zero, etc.

- Convé explorar la possibilitat d'emprar tècniques que permetin fer càlculs de forma distribuïda, de manera que cada agent que intervé en la computació mantingui les seves dades (*secure multiparty computation SMPC)*. En una línia similar, quan es desenvolupen models amb intel·ligència artificial convé adoptar mecanismes d'aprenentatge federat, de manera que les persones que tenen les dades (individus, entitats, etc.) poden entrenar el model de forma distribuïda, sense que hagin de cedir les dades a una entitat que centralitza l'entrenament.

3.6 Manteniment i conservació de les dades

En aquest apartat, ens referirem tant a les mesures que cal adoptar per garantir la confidencialitat, la integritat i la disponibilitat de la informació com a la limitació del termini de conservació.

3.6.1 Confidencialitat, integritat i disponibilitat de la informació

Cal garantir la seguretat de la informació. Essencialment, això implica que la informació personal no pot ser accessible a persones no autoritzades (**confidencialitat**), no es pot alterar indegudament (**integritat**) i ha d'estar disponible quan es necessiti (**disponibilitat**).

Aquestes tres característiques es poden protegir amb diferents mesures, que cal determinar d'acord amb la probabilitat i la gravetat dels riscos existents.

La confidencialitat, la integritat i la disponibilitat són diferents dimensions de seguretat que, malgrat que estant vinculades, poden requerir algunes mesures diferents. Per això, a continuació es presenten diferents mesures agrupades en relació amb les diverses dimensions de seguretat, si bé cal tenir en compte que algunes mesures poden respondre a la vegada a més d'una d'aquestes dimensions. Per exemple, quan s'evita l'accés indegut a la informació (confidencialitat), s'està contribuint també a protegir-ne la integritat o la disponibilitat (per exemple, dificultant-ne el segrest). En definitiva, si bé s'opta per aquesta estructura separada a efectes expositius, cal tenir present que la seguretat és un concepte integral.

Confidencialitat i integritat

Per garantir la confidencialitat i la integritat, és imprescindible establir controls d'accés a la informació.

Aspectes rellevants

- Cal establir una **política de permisos** que atorgui únicament els permisos operatius indispensables. Cal definir rols de manera que cada persona usuària només disposi dels permisos imprescindibles per exercir les seves funcions (principi de la necessitat de conèixer). Fins i tot si es tracta d'un alt directiu de l'organització responsable del tractament, no hauria de tenir permisos il·limitats si la seva tasca ordinària no ho requereix, sens perjudici que se li pugi atorgar puntualment si en algun moment cal.

- Per identificar les persones usuàries es poden demanar **certificats** electrònics, que ofereixen un alt grau de robustesa. No obstant això, quan l'exigència d'aquest mitjà no sigui proporcionada o adequada per altres motius, cal aplicar altres mecanismes d'identificació, com ara els de clau concertada.[15]

[15] En el cas de les administracions públiques, l'article 9 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques regula els mitjans d'identificació electrònica dels ciutadans.

- Si és possible i proporcionat en termes de seguretat versus usabilitat, convé establir un sistema basat en **múltiples factors d'autenticació**. Els sistemes basats en un únic factor (com ara contrasenya) de vegades es poden vulnerar fàcilment (per exemple, per una mala custòdia, la poca robustesa o l'espionatge de reüll o *shoulder surfing*). En aquest sentit, es recomana aplicar sistemes de doble factor que han de combinar aspectes diferents, entre (i) alguna cosa que sé (contrasenya), (ii) alguna cosa que tinc (testimoni o telèfon mòbil) o (iii) alguna cosa que soc (aspectes biomètrics).

Sobre la possibilitat d'emprar dades biomètriques, cal advertir que són dades de categoria especial, de manera que només es poden emprar si hi concorre alguna de les excepcions que preveu l'RGPD[16] i quan fer-ne ús sigui proporcionat. Per tant, es recomana que no s'opti per aquesta possibilitat, tret que sigui estrictament necessari.

- **Gestió de les claus d'accés**: l'atorgament de claus d'accés a les persones que han d'accedir a la informació, ja siguin les usuàries últimes del servei o les encarregades de gestionar l'aplicació, ha de tenir en compte diversos aspectes que afecten tant les característiques de la clau com el procediment de creació, gestió i recuperació.

- **Credencials segures:** l'exigència de contrasenyes robustes protegeix d'atacs de password guessing[17] o de diccionari i força bruta[18]: per això, convé que sigui la mateixa aplicació la que exigeixi un nombre mínim de caràcters, majúscules, minúscules i caràcters especials.

Atesa la importància d'emprar una clau prou robusta, quan l'usuari la configura és recomanable que el sistema no només li indiqui el nivell de robustesa de la clau que està proposant, sinó que impedeixi establir-la si no compleix determinats requisits de solidesa.

Convé no utilitzar contrasenyes establertes per defecte en béns o serveis.

Per fer front a aquests eventuals atacs, també es poden implantar mesures com ara:

1. Bloqueig de l'usuari, en cas de múltiples intents fallits d'accés: es bloqueja el perfil o la IP, un cop hi ha hagut un determinat nombre d'intents fallits dins d'un període de temps prèviament definit.

[16] Vegeu l'article 9.2 de l'RGPD.
[17] *Password guessing*: pot ser protagonitzat per algú que coneix la víctima potencial i per tant pot intuir la paraula de pas, o bé per professionals que, mitjançant tècniques d'Open Source Intelligence – OSINT –, també poden conèixer dades com la data de naixement, la identitat dels fills, etc., que sovint s'utilitzen per crear contrasenyes.
[18] Atacs "de diccionari" o de força bruta consistents en múltiples intents consecutius.

2. Introducció d'un CAPTCHA en el procés de validació.

- El **procés de generació i,** si escau, **de comunicació** de la contrasenya ha de garantir que únicament la persona usuària coneix les claus.
- La solució tecnològica s'ha de configurar de manera que el responsable hagi d'emmagatzemar les **credencials d'accés dels usuaris** mitjançant una empremta electrònica (*hash*) de la contrasenya.
- Convé establir un mecanisme que en forci la **renovació periòdica**.
- Cal configurar l'aplicació o web perquè **la sessió dels usuaris es tanqui de manera automàtica, transcorregut un determinat període de temps** d'inactivitat. També perquè **s'invalidin les galetes que guarden la sessió,** de manera que per accedir-hi de nou calgui tornar a identificar-se.
- Cal disposar d'un **registre d'accessos i d'activitat** que permeti analitzar detalladament i retrospectivament qualsevol circumstància que pugui afectar la informació. Disposar d'un registre d'accessos té múltiples beneficis, ja que en si mateix és un element dissuasiu, pot contribuir a detectar actuacions anòmales o sospitoses i, si s'ha produït alguna actuació indeguda, permet recollir evidències sobre què ha succeït efectivament. Les evidències poden servir per adoptar les mesures correctores internes o externes (inclosa la notificació d'una violació de seguretat, perquè els usuaris puguin protegir-se adequadament), així com per exigir les responsabilitats escaients.

Més enllà del control d'accessos, també és oportú considerar altres aspectes que contribueixen decisivament a preservar la confidencialitat i la integritat i que fan referència a "com" s'emmagatzema la informació.

Aspectes rellevants

- Cal assegurar que la informació es manté **xifrada** sempre que sigui possible.
- Cal emprar signatura electrònica quan sigui possible, com a garantia de l'autoria, la data i hora i la integritat del document.
- Cal vetllar que els processos d'anonimització i pseudonominització que s'emprin no han perdut efectivitat.

Addicionalment, també és convenient fer proves de penetració que permetin identificar possibles vulnerabilitats, així com incloure algun sistema de monitorització d'incidents que permeti detectar ràpidament qualsevol anomalia.

Aspectes rellevants

- Cal preveure **proves periòdiques** que comprovin possibles vulnerabilitats en la protecció de la confidencialitat de la informació davant d'atacs externs. Principalment, hi ha tres tipologies d'auditories de seguretat externes: (i) caixa negra – quan l'auditor intenta accedir-hi sense cap coneixement previ del sistema o aplicació – (ii) caixa blanca – quan l'auditor parteix d'un coneixement complet del sistema o servei a analitzar - i (iii) caixa gris – quan es facilita algun tipus d'informació a l'auditor que ha d'intentar l'atac-. En general, és recomanable fer proves de caixa negra, ja que se simula un escenari el màxim realista possible d'algú extern que no té coneixements previs del sistema que s'està verificant. No obstant això, puntualment pot ser interessant proporcionar a la persona auditora algunes informacions que li permetin simular atacs a partir de diferents nivells de privilegi d'usuari.

- Pot resultar especialment oportú **auditar el propi codi,** per detectar possibles riscos de seguretat.[19]

- Cal instaurar mecanismes adequats per **identificar comportaments anòmals o fuites de dades,** si és possible de manera automatitzada, que facin possible una reacció ràpida i adequada. Per exemple, mitjançant mesures que controlin el trànsit de la informació i que permetin detectar qualsevol comportament anòmal i alertar els responsables del dispositiu o servei.

Finalment, cal assenyalar que és important adoptar qualsevol altra mesura de seguretat **adequada als riscos existents.**[20]

[19] Únicament a tall d'exemple, hi ha productes que permeten automatitzar aquest tipus d'auditories. En concret, es tractaria de verificar, per exemple, que l'accés a les bases de dades s'ha dissenyat tenint en compte que no s'hi pugui accedir indegudament mitjançant atacs de XXSS (validant els camps d'*input* abans que s'executin a la mateixa base de dades).

[20] En el cas del sector públic, a l'Estat expanyol cal tenir en compte l'Esquema Nacional de Seguretat (ENS), aprovat pel Reial decret 311/2022, de 3 de maig. Tot i això, cal tenir present que l'ENS indica expressament – en virtut del seu art. 3 – que prevalen les mesures derivades d'una anàlisi de risc relatiu específicament executat tenint en compte la protecció de les dades personals.

Disponibilitat

Aspectes rellevants

- Cal establir mecanismes automatitzats per obtenir **còpies de seguretat** periòdicament i en diferent ubicació. Tot i que conèixer determinades circumstàncies que en un tractament concret poden afectar la disponibilitat (talls elèctrics, manca de connectivitat, incendis, inundacions, obsolescència de determinades parts del sistema d'informació preexistent, etc.) pot sobrepassar l'àmbit que correspon als desenvolupadors, cal que en tinguin un coneixement exhaustiu a l'hora d'establir en una aplicació el sistema d'obtenció de còpies i el sistema de recuperació. El mecanisme (còpies periòdiques, servidor mirall, etc.) i la freqüència de les còpies dependrà de la probabilitat i la gravetat derivades d'una pèrdua de disponibilitat. Sovint, es fa referència a la regla 3-2-1: disposar de tres còpies de seguretat, almenys en dos suports diferents i una de les còpies fora de l'entorn de treball (aïllada).

- Perquè aquest plantejament sigui efectiu, cal configurar **accessos diferents a les còpies de seguretat**. En cas contrari, si les credencials d'un administrador del sistema es veuen compromeses, l'atacant podria accedir tant a la informació viva com a la corresponent a les diferents còpies i, en conseqüència, podria corrompre-ho tot alhora.

- Cal preveure proves periòdiques del procediment de recuperació, per garantir la disponibilitat de la informació i la continuïtat dels serveis.

- Atès que la disponibilitat també depèn d'elements com (i) maquinari (ii) subministraments com ara l'electricitat i (iii) de connectivitat, és recomanable valorar la possibilitat de redundar aquests aspectes crítics.

3.6.2 Limitació del termini de conservació

Les dades només s'han de conservar durant el temps necessari per assolir la finalitat perseguida.

Transcorregut aquest temps, s'han de suprimir.

La supressió no equival a l'eliminació, sinó que dona lloc al bloqueig[21] durant el termini en què calgui conservar-les per atendre eventuals responsabilitats. Un cop finalitzat el període de bloqueig, les dades s'han de destruir o, si escau, anonimitzar.

[21] El bloqueig consisteix en la identificació i la reserva de les dades, amb mesures tècniques i organitzatives per impedir-ne el tractament, inclosa la visualització, tret de la posada a disposició de les dades als jutges i tribunals, el ministeri fiscal o les

Les dades que es vulguin conservar amb finalitats estadístiques o similars no s'han de mantenir -de manera que permetin identificar les persones afectades- més temps de l'estrictament necessari per complir la finalitat del tractament.

Mesures

- Abans d'iniciar la recollida de les dades, cal determinar-ne el termini de conservació (inclòs el període de bloqueig) i informar-ne les persones afectades.[22]
- Cal establir mecanismes automatitzats de supressió de les dades innecessàries.
- Convé establir mecanismes que permetin bolquejar les dades suprimides o rectificades, mentre siguin necessàries per atendre les eventuals responsabilitats, i en facilitin la destrucció un cop finalitzi el període de bloqueig.
- Si es volen conservar les dades amb finalitats estadístiques més enllà del període de conservació establert, cal aplicar mesures adequades com ara l'anonimització de la informació.
- Cal aplicar mètodes que assegurin una eliminació efectiva de la informació que no s'hagi de conservar. En particular, cal esborrar els fitxers i les unitats de forma segura (sobreescrivint la informació repetides vegades) o, fins i tot, en el cas de dispositius que no s'hagin d'utilitzar (discs durs, memòries USB, etc.), amb la destrucció física, especialment quan surtin del control de l'organització.
- Convé minimitzar el temps que es guarda la informació de navegació a l'equip de l'usuari. És preferible utilitzar galetes de sessió que galetes persistents i, si s'utilitzen, fixar-ne una data de caducitat. Així mateix, cal evitar l'ús de mecanismes d'emmagatzematge que busquen evitar guardar dades sense que l'usuari en tingui cap control. Per exemple, les zombie cookies, que utilitzen diverses tècniques per regenerar-se quan l'usuari les esborra.

administracions públiques competents. En particular, de les autoritats de protecció de dades, per exigir possibles responsabilitats derivades del tractament mentre no hagin prescrit (art. 32 LOPDGDD).

[22] En l'àmbit de les administracions públiques catalanes cal tenir en compte els terminis de conservació establerts a les taules d'avaluació documental.

4. Mesures clau per protegir les dades personals

En aquesta guia s'han esmentat diferents mesures que contribueixen a millorar la protecció de la informació personal, en alguna o en diverses fases del tractament.

Sens perjudici d'això, en aquest apartat es fa referència a tres mesures que, per la seva rellevància, estan previstes de manera específica al reglament europeu de protecció de dades. Es tracta del xifratge, l'anonimització i la pseudonimització.

Atès que aquestes mesures impliquen un benefici clar per a la protecció de les dades personals, formen part del conjunt més ampli que en l'àmbit de la protecció de dades es coneix com a PET (*privacy enhancing technologies*) o tecnologies que milloren la privacitat.

4.1 Xifratge

El xifratge és un procés que transforma una informació (text en clar), de manera que no sigui comprensible (text xifrat). El xifratge es fa d'acord amb una clau de xifratge i només qui té la clau de desxifratge pot revertir el procés i accedir a la informació. En qualsevol cas, les dades personals xifrades continuen essent dades personals sotmeses a la normativa de protecció de dades personals.

Els sistemes de xifratge s'acostumen a classificar d'acord amb el mètode emprat per xifrar i desxifrar la informació:

- **Criptosistemes simètrics o de clau privada**: s'empra la mateixa clau per xifrar i per desxifrar.

- **Criptosistemes asimètrics o de clau pública**: s'utilitzen claus diferents per xifrar i per desxifrar. En aquest supòsit, l'usuari té dues claus (pública i privada). Quan es vol trametre un missatge o comunicació a un altre usuari, el missatge es xifra amb la clau pública del receptor, de manera que només ell (que és l'únic que té la seva clau privada) el podrà desxifrar.

El gran avantatge dels sistemes de clau pública és que les parts que es volen comunicar una informació de forma secreta no han de compartir en cap moment la seva clau privada. D'altra banda, aquest sistema sí que exigeix un mecanisme perquè les diferents parts comparteixin la seva clau pública de forma segura. Això es fa amb certificats digitals, en què una entitat reconeguda dona fe de la validesa d'una clau; és el que es coneix com a infraestructura de clau pública (PKI).

Atès l'alt cost computacional dels criptosistemes de clau pública (derivats de la complexitat de les operacions matemàtiques que són necessàries) també hi ha la possibilitat dels criptosistemes híbrids, en els quals el text en clar es xifra amb un algorisme de clau privada, amb una clau generada aleatòriament. Al seu torn, aquesta clau es xifra amb un algorisme de clau pública i s'adjunta al missatge. El destinatari desxifrarà la clau utilitzant la seva clau privada i, així, podrà desxifrar el text.

El xifratge constitueix una actuació especialment recomanable per protegir les dades personals, tant des del punt de vista de la confidencialitat com de la integritat. I això fins al punt que la normativa de protecció de dades considera que no cal notificar una violació de seguretat de les dades a l'autoritat de control, ni comunicar-la a les persones afectades, si s'han adoptat mesures que facin inintel·ligibles les dades per qualsevol persona que no hi estigui autoritzada, com ara el xifrat.

Sens perjudici del que resulti de l'anàlisi de riscos, és especialment recomanable xifrar la informació quan es tracta una gran quantitat d'informació o dades especialment sensibles, ja siguin de categoria especial o altres dades (com ara dades econòmiques). En qualsevol cas, com qualsevol mesura de protecció ha de ser proporcionada als riscos existents, de manera que aplicar aquesta mesura hauria de comportar uns beneficis superiors als costos d'implementar-la.

Si les dades xifrades s'han de sotmetre a operacions o càlculs, pot ser d'especial utilitat el xifratge homomòrfic, que permet fer determinades operacions algebraiques sobre dades xifrades. Això pot ser útil, per exemple, quan es guarden dades sensibles al núvol i es vol operar sobre elles.

És important tenir en compte que els processos de xifratge comporten sempre un cert risc de desxifratge. Aquests riscos poden ser computacionals (els algorismes de xifratge esdevenen progressivament obsolets) o associats a la gestió i conservació de les claus emprades per xifrar i desxifrar la informació. En aquest sentit, es recomana revisar[23] al llarg del temps la robustesa de l'algorisme i, també, que les claus es generin i es custodiïn de forma segura.

Hi ha altres mecanismes criptogràfics que permeten obtenir diferents funcionalitats i que, per tant, també cal valorar a l'hora de desenvolupar una aplicació, com ara la signatura electrònica, les funcions d'empremta electrònica (*hash*), esquemes de compartició de secrets, etc.

4.2 Anonimització

Es tracta d'un procés que té com a objectiu impedir que es puguin identificar persones físiques dins d'un conjunt de dades, sense esforços desproporcionats, ja sigui directament o indirectament; per tant, és un procés irreversible. Com que les dades deixen de ser atribuïbles a persones físiques, perden la consideració de dades personals. En conseqüència, els riscos per a les persones afectades disminueixen i la normativa de protecció de dades personals deixa de ser d'aplicació.

[23] Per exemple, el Centre Criptològic Nacional (CCN) publica recurrentment informació i guies que poden ser útils. Així, el maig de 2022 s'ha publicat la Guia de seguretat CCN-STIC 807 "Criptología de empleo en el Esquema Nacional de Seguridad".

Abans d'iniciar qualsevol tractament, és recomanable analitzar si es pot dur a terme sense emprar dades personals o utilitzant dades anonimitzades. Si és així, cal optar per aquesta possibilitat.

Cal tenir present que el procés d'anonimització en si mateix és un tractament de dades personals. Per tant, durant aquesta fase cal tenir en compte la normativa de protecció de dades personals.

Així mateix, en el procés d'anonimització cal establir una separació funcional, de manera que les persones que hi intervenen no coincideixin amb les que estan vinculades al tractament de les dades un cop ja han estat anonimitzades.

Les tècniques d'anonimització alteren les dades per protegir la privacitat. Això té, inevitablement, un efecte sobre la utilitat de les dades.

4.2.1 Tècniques d'anonimització

Les tècniques d'anominització es classifiquen en dues grans categories, d'acord amb el procediment emprat: emmascarament i generació de dades sintètiques.

Tècniques d'emmascarament

Les tècniques d'emmascarament parteixen de les dades originals i les modifiquen. Es manté una relació entre els registres de dades originals i els registres de dades emmascarats. Aquesta relació fa que el risc de reidentificació s'hagi de tenir molt en compte.

El ventall de tècniques d'emmascarament és molt ampli.[24] Segons com afecta a la veracitat de les dades, aquestes tècniques es classifiquen en pertorbatives i no pertorbatives. Les pertorbatives n'alteren la veracitat. Per exemple, són tècniques d'emmascarament pertorbatiu:

- **Afegir soroll**. S'afegeix un cert nivell de soroll aleatori a les dades originals perquè els valors no siguin exactes. El risc associat a aquestes dades dependrà del nivell de soroll afegit. Com més gran sigui, més incertesa tindrem sobre les dades originals i, per tant, el risc serà menor.

- **Microagregació**. Consisteix a agrupar els registres en grups, amb una cardinalitat mínima fixada, i reemplaçar cadascun dels grups per un nou registre que sigui representatiu del grup. D'aquesta manera, els registres de les dades anonimitzades

[24] Per a més informació: A Network of Excellence in the European Statistical System in the field of Statistical Disclosure Control.

ja no es corresponen a una persona concreta, sinó que fan referència a un grup de persones. Com més grans siguin els grups, menor serà el risc.

- **Intercanvi de rang**. Es tracta de reemplaçar el valor d'un atribut d'un registre pel valor d'un altre registre que està dins d'un rang del valor inicial. A diferència de l'addició de soroll, en l'intercanvi de rang es preserva la distribució de dades en cada atribut.

Cada tècnica d'emmascarament té alguna propietat que la pot fer més adient que una altra, en una situació concreta. Ara bé, cal tenir sempre present que aquestes tècniques alteren la veracitat de les dades. Des del punt de vista de la privacitat això és positiu perquè, encara que es reidentifiqui un registre, hi hauria incertesa sobre la veracitat de les dades que conté. D'altra banda, aquesta pèrdua de veracitat de les dades, fa que aquestes tècniques no es puguin emprar en determinades situacions.

Per mantenir la veracitat de les dades es poden emprar tècniques d'emmascarament no pertorbatiu, que redueixen la granularitat de la informació de manera que no es pugui reidentificar un registre. Per exemple, són tècniques d'emmascarament no pertorbatiu:

- **Supressió**. Consisteix a eliminar determinades dades, de manera que la persona afectada ja no sigui identificable. La supressió és molt comuna amb les variables identificatives; les variables identificatives, en general, no aporten gaire valor estadístic i, per tant, suprimir-les no acostuma a ser problemàtic. D'altra banda, la reidentificació també es pot produir per la combinació de diferents atributs que, per si sols, no són identificadors (aquestes combinacions d'atributs es coneixen com a quasi-identificadors). Per evitar la reidentificació, cal suprimir els quasi-identificadors que poden permetre identificar persones concretes.

- **Generalització (o recodificació global)**. Consisteix a reemplaçar la informació en una variable o atribut de manera que el nou valor correspongui a una categoria més ampla. Per exemple, es pot reemplaçar l'edat amb rangs d'edat.

Generació de dades sintètiques

Amb les tècniques de generació de dades sintètiques s'obtenen dades noves a partir d'un model de les dades originals. No hi ha una relació directa entre les originals i les sintètiques.

La idea és que el model ha de preservar les propietats estadístiques de les dades que interessa analitzar. Cal tenir en compte que les dades sintètiques només recullen determinades propietats. Per tant, l'ús d'aquest tipus de dades pot limitar la tipologia de les anàlisis que es poden fer.

El fet que les dades sintètiques no reprodueixin les dades originals aïlladament considerades fa que es consideri una tècnica segura contra el risc de reidentificació. Ara bé, aquest fet, com també el risc de revelació, depèn del model que s'ha utilitzat. Un model massa precís pot comportar uns riscos elevats. Si el model consisteix únicament en algunes propietats estadístiques de les dades originals que volem preservar, el risc de reidentificació pot estar controlat. Ara bé, la utilització de models molt complexos pot donar lloc a un sobreajustament; és dir, que el model no sigui una representació de les propietats

estadístiques de les dades originals, sinó que representa dades concretes. En aquest cas, el risc de reidentificació pot ser alt.

Per tant, determinar les propietats de les dades que interessa tractar és crític. Per exemple, en la fase de desenvolupament i proves, pot ser que n'hi hagi prou de preservar la validesa sintàctica i semàntica de les dades (és a dir, que tinguin els tipus adequats i que no hi hagi combinacions sense sentit). Unes dades generades d'aquesta manera eviten qualsevol risc.

4.2.2 Riscos en l'anonimització

Els processos d'anonimització no garanteixen de manera absoluta que sigui impossible esbrinar informació personal a partir de les dades anonimitzades. Un cop aplicades les tècniques descrites anteriorment, cal avaluar quin és el nivell de risc i ajustar l'anonimització.[25]

Moltes tècniques d'anonimització es basen en suposicions sobre la informació disponible per a un eventual atacant. Com més informació tingui, més fàcil serà, per exemple, que pugui reidentificar un registre. Pot ser molt difícil determinar quina és la informació disponible externament i, a més, aquesta informació pot canviar amb el pas del temps, per la qual cosa cal avaluar els riscos existents en cada moment.

En els processos d'anonimització que s'acaben de descriure, hi ha models de privadesa que busquen donar unes garanties de privacitat ja en el moment de fer l'anonimització. D'aquesta manera, primer es fixa el risc i, després, s'aplica una tècnica d'anonimització per assolir-lo.

Entre els models de privadesa més coneguts hi ha el k-anonimat (i els seus models relacionats, com ara l-diversitat i t-proximitat) i la privadesa diferencial.

K-anonimat

El k-anonimat tracta amb el risc de reidentificació fent que cada registre es pugui associar a un conjunt de k persones. El k-anonimat assumeix que les reidentificacions es produeixen a través d'un conjunt d'atributs (els quasi-identificadors) i exigeix que cada combinació d'aquests quasi-identificadors que aparegui a les dades anonimitzades es repeteixi, com a mínim, k vegades.

Les formes més habituals d'obtenir k-anonimat són:

- **Generalització i supressió**. Es redueix la granularitat de la informació en els quasi-identificadors, de manera que cada combinació de valors present a les dades anonimitzades es repeteixi k vegades.

[25] En relació amb l'efectivitat de l'anonimització, es pot consultar el capítol 2 "How do we ensure anonymisation is effective" de la guia sobre anonimització, pseudonimització i tecnologies d'ampliació de la privacitat anonimització, pseudonimització i tecnologies d'ampliació de la privacitat (PET en les seves sigles en anglès) que està confeccionant la *Information Commissioner's Office*.

- **Microagregació**. S'aplica microagregació sobre els quasi-identificadors amb grups de mida k.

El k-anonimat pot acabar permetent la identificació de persones concretes, quan la variabilitat d'un atribut en un grup de registres k-anònim és petita. Per evitar aquest problema, s'han desenvolupat altres models de privadesa, com ara la l-diversitat i la t-proximitat, que exigeixen una variabilitat mínima.

Privacitat diferencial

La privacitat diferencial és un model de privacitat per a les consultes a bases de dades. És a dir, no es genera una nova base de dades anonimitzada que es pot analitzar, sinó que les consultes es fan sobre la base de dades original i s'altera el valor de la resposta per protegir la privacitat.

La privacitat diferencial és reconeguda per donar fortes garanties de protecció de la privacitat que, a més, són independents de la informació disponible externament. Ara bé, l'aplicació estricta de la privacitat diferencial presenta moltes limitacions pel gran impacte que té sobre la utilitat de les dades. Per exemple, la privacitat diferencial s'utilitza al cens dels EUA, però per mantenir la utilitat de les dades, cal aplicar uns paràmetres tan extrems que es perden totes les garanties[26].

4.3 Pseudonimització

La pseudonimització és un procés mitjançant el qual deixa de ser possible identificar la persona física a qui corresponen les dades si no es recorre a informació addicional que ha d'estar emmagatzemada per separat i subjecta a mesures tècniques i organitzatives per evitar la reidentificació de les persones interessades[27]. És a dir, només qui ha fet la pseudonimització pot acabar relacionant la informació amb persones identificades o identificables. En canvi, les terceres persones no poden establir aquesta relació.

A diferència de l'anonimització, la pseudonimització és un procés reversible. Les dades personals pseudonimitzades continuen essent dades personals i, per tant, els és d'aplicació la normativa de protecció de dades.

Algunes de les tècniques per fer efectiva la pseudonimització són:

- Ús de pseudònims: només qui tingui la correspondència entre el pseudònim i la identitat real ha de poder atribuir la informació a la persona individual.
- Ús de codis aleatoris que no siguin previsibles per a terceres persones.

[26] Diferential Privacy for census data explained.

[27] Per aquest motiu les dades resultants de la pseudonimització es continuen considerant dades personals i, per tant, romanen subjectes a les obligacions de l'RGPD. Tanmateix, la normativa europea fomenta l'ús de pseudònims en el tractament de dades personals. A més, l'RGPD considera que la pseudonimització permet reduir els riscos per a les persones interessades i contribuir al compliment de la normativa

- El xifratge habitualment també es considera una tècnica de pseudonimització, atès que el procés és reversible mitjançant l'ús d'una clau.

Com en el cas de l'anonimització, perquè la pseudonimització desplegui tota la seva eficàcia convé establir una separació funcional, de manera que les persones que intervenen en el procés de pseudonimització no coincideixen amb les que estan vinculades al procés del tractament de les dades un cop ja han estat pseudonimitzades. També cal tenir present que els processos de pseudonimització no garanteixen al 100% que terceres persones no puguin acabar reidentificant les persones afectades, per la qual cosa cal analitzar aquest risc i revisar-lo periòdicament.

Cal fer referència també a la possibilitat en determinats contextos (per exemple, xarxes socials, metavers, etc.) de recórrer a la utilització d'identitats digitals diferenciades de la identitat real. L'ús de d'àlies o avatars, tot i que no són pròpiament una tècnica de pseudonimització, pot ser especialment útil per preservar un cert grau de privacitat, atès que no deixa de ser una capa de protecció entre la identitat real de l'usuari i les seves actuacions en l'ecosistema digital amb aquestes altres identitats. No obstant això, aquest mecanisme no constitueix una garantia d'anonimització, ni tan sols de pseudonimització, atès que segons el context i la informació associada es pot acabar identificant la persona afectada. Per tant, són dades personals.

5. Normativa de protecció de dades

Normativa general

Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (RGPD).

Llei orgànica 3/2018, de 5 de de desembre, de protecció de dades personals i garantia dels drets digitals (LOPGDD)

Llei orgànica 7/2021, de 26 de maig, de protecció de dades personals tractades per fins de prevenció, detecció, investigació i enjudiciament d'infraccions penals i d'execució de sancions penals (LOPDSPJP).

Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS).

Altres normes

Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (LSSICE) (arts. 21, 22, 38.3 *c*, *d* i *i*, 38.4 *d, g* i *h*, 43.1.

6. Bibliografia

Privacitat des del disseny i per defecte

Privacy by Design. The 7 Foundational Principles. Ann Cavoukian. Ph.D. Information and Privacy Commissioner, Ontàrio, Canadà.

Privacy Design Strategies (The Little Blue Book), JAAP-HENK HOEPMAN (2022).

Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices. (2012) Ann Cavoukian, Ph.D.

Directrius 4/2019 relatives a l'article 25. Protecció de dades des del disseny i per defecte. (versió 2.0, 2020). Comitè Europeu de Protecció de Dades.

Data protection by design and by default. Information Commissioner's Office (ICO).

Guia RGPD CNIL de l'equip de desenvolupament. Commission Nationale d'Informatique et des Libertés (CNIL).

Directrius Desenvolupament de programari amb protecció de dades per disseny i per defecte, (2017). Autoritat de protecció de dades de Noruega.
Guía de privacidad desde el diseño. Agència Espanyola de Protecció de Dades (AEPD).

Guía de protección de datos por defecto. Agència Espanyola de Protecció de Dades (AEPD).

Protecció de dades des del disseny i protecció de dades per defecte. Garante per la Protezioni dei Dati Personali (GPDP).

Informe *"*Enginyeria de protecció de dades. De la teoria a la pràctica*"* (2022). ENISA.

Informe Privadesa i protecció de dades des del disseny: des de la política fins a l'enginyeria (2014). ENISA.

Altres recursos

Dictamen 02/2013 sobre les aplicacions dels dispositius intel·ligents, (2013). Grup de treball l'article 29 sobre protecció de dades.

Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them (v. 1.0). Comitè Europeu de Protecció de Dades.

Deceptive design. Harry Brignull.

PETs Maturity Assessment Repository (2019). ENISA.

Protecting privacy in practice. (2019). The Royal Society.

Privacy patterns. Privacy Patterns.org.

Web Security Testing Guide. Open Web A*pplication Security Project (OWASP).*

Cross Site Scripting Prevention Cheat Sheet. Open Web Application Security Project (OWASP).

Dictamen 5/2014, sobre tècniques d'anonimització. Grup de Treball de l'article 29.

Data Pseudonymisation: Advanced Techniques and Use Cases (2021). ENISA.

Anonymisation, pseudonymisation and privacy enhancing technologies guidance. (2021). Information Commissioner's Office (ICO).

Orientaciones y garantías en los procedimientos de anonimización de datos personales. Agència Espanyola de Protecció de Dades (AEPD).

Introducción al Hash como técnica de seudonimización de datos personales. Agència Espanyola de Protecció de Dades (AEPD).

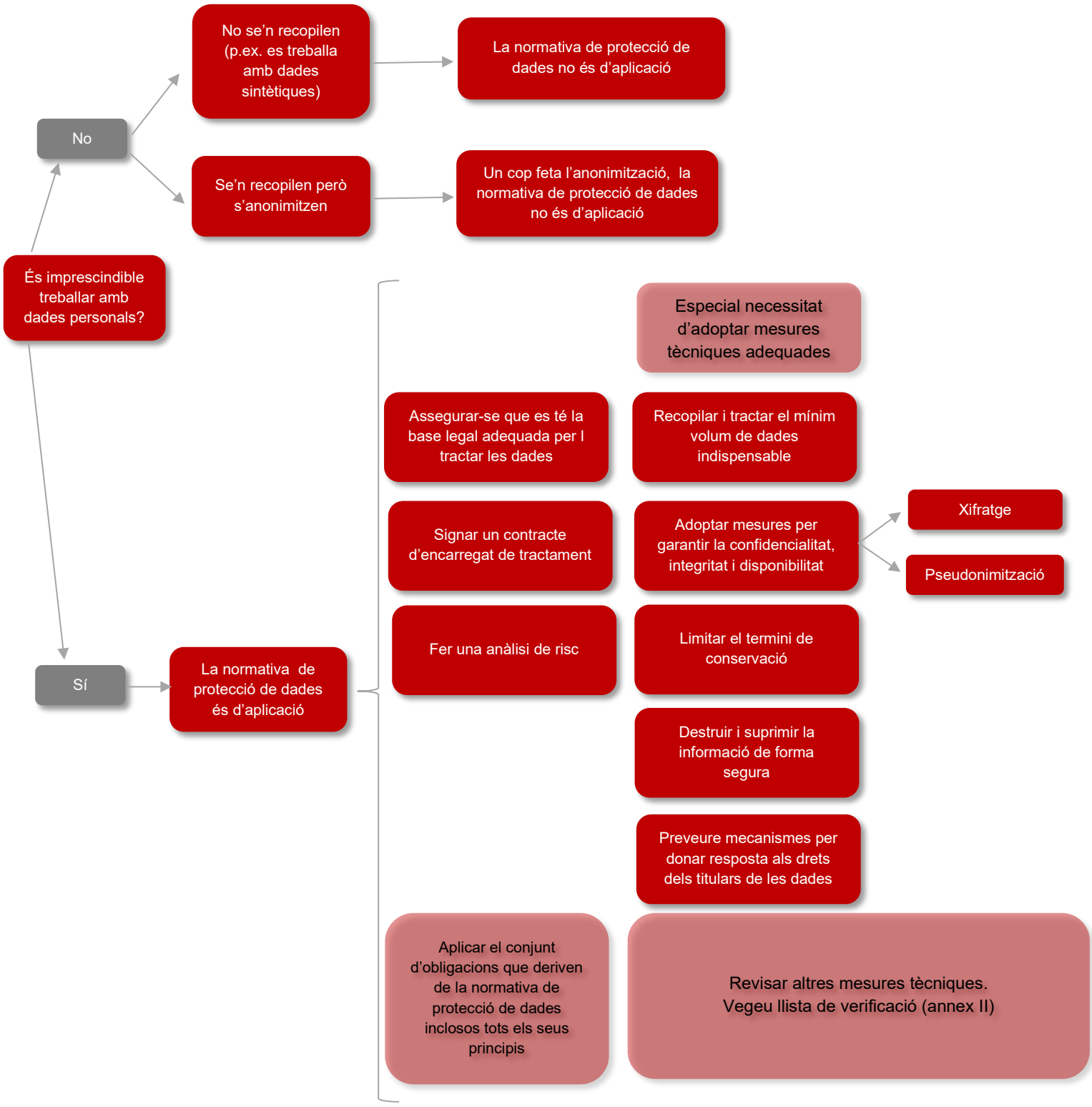
10 malentendidos relacionados con la anonimización. Agència Espanyola de Protecció de Dades (AEPD).

Cifrado y Privacidad III: Cifrado Homomórfico (2020). Agència Espanyola de Protecció de Dades (AEPD).

Guia pràctica Avaluació d'impacte relativa a la protecció de dades (2019). Autoritat Catalana de Protecció de Dades (APDCAT).

Guidance on AI and data protection. Information Commissioner's Office (ICO)

Annex I. Anàlisi prèvia



Annex II. Checklist

Fase de disseny

☐ Introduir estratègies de disseny per garantir la protecció de les dades
☐ Aplicar patrons de privacitat

Fase de desenvolupament i de proves

☐ Signar un contracte d'encàrrec del tractament si el desenvolupador o un tercer contractat per aquest han d'accedir a dades personals.
☐ Separar adequadament els entorns de producció i el de desenvolupament i proves.
☐ Valorar la possibilitat de treballar amb dades fictícies, en entorns de proves.
☐ Minimitzar la quantitat de dades recollides ja en la fase de proves.
☐ Valorar la possibilitat d'anonimitzar o pseudinomitzar les dades recollides en la fase de proves o utilitzar dades sintètiques.
☐ Garantir que la ubicació on s'allotja o es tracta la informació és en un país que ofereixi garanties adequades.
☐ Emprar el protocol wifi que proporcioni un major grau de seguretat.
☐ Revisar la qualitat del codi emprat i seguir les recomanacions de les guies de programació segura.
☐ Fer una anàlisi de riscos per determinar les mesures de seguretat.
☐ Preveure la formació del personal per garantir, en tot moment, la minimització de riscos.

Recollida de les dades

☐ Recollir només les dades imprescindibles. Això afecta: :
- Dades recollides mitjançant formularis.
- Dades tècniques que es recopilin (IP, MAC, geolocalització, etc...).
- Codi inserit que pugui transferir informacions.
- Altres vies de recollida de dades.

☐ Valorar la possibilitat d'anonimitzar o pseudonimitzar les dades personals recollides.
☐ Minimitzar especialment la recollida de categories especials de dades.
☐ Distingir clarament la informació que s'ha de proporcionar obligatòriament de la que és opcional.
☐ Demanar només els permisos per accedir i recollir informació que siguin rellevants per a la finalitat que persegueix.
☐ Valorar la possibilitat que el tractament es faci directament als dispositius dels usuaris.
☐ Informar adequadament les persones afectades sobre com es tractaran les seves dades.
☐ Fer còpies de les clàusules informatives existents en cada moment, aplicant un segell de temps verificable (*timestamp*).
☐ Abstenir-se d'implementar patrons foscos (*dark patterns*).
☐ Verificar que es compleixen els requisits perquè el consentiment, si cal, sigui vàlid:
- Les caselles no poden estar remarcades.
- El consentiment ha de ser diferent per a cada finalitat.
- No hi pot haver vinculació o condicionament entre consentiments.

- Establir mecanismes que permetin verificar la identitat de qui presta el consentiment.
- Verificar la identitat i l'edat de la persona que atorga el consentiment.
- El consentiment s'ha de poder revocar amb mecanismes de complexitat equivalent als emprats per atorgar-lo.

☐ Conservar evidències del consentiment obtingut.

Ús de les dades

☐ Implementar mecanismes que permetin classificar adequadament la informació, d'acord amb les finalitats i els tractaments a què s'han de sotmetre.
☐ Incorporar mesures que facilitin l'exercici i l'atenció dels drets.

Comunicació o divulgació de les dades

☐ Quan la difusió es basa en el consentiment de la persona afectada, cal establir mecanismes perquè, per defecte, les dades no siguin accessibles a terceres persones.
☐ Establir controls sobre qui accedeix a la informació.
☐ Preveure'n la despublicació automatitzada un cop es compleixin els terminis d'ús de la informació.
☐ Incloure el xifratge d'extrem a extrem en les comunicacions i, si escau la possibilitat d'emprar connexions VPN.
☐ Emprar protocols https per a serveis via web.
☐ Analitzar la possibilitat de comunicar les dades xifrades.
☐ En la fase de desenvolupament i aprenentatge de models d'intel·ligència artificial aplicar sistemes d'aprenentatge federat.

Manteniment i conservació de les dades

Confidencialitat i integritat

☐ Establir una política de permisos adequada.
☐ Explorar l'opció de requerir com a mecanismes d'identificació i autenticació:

- L'ús de certificats electrònics
- Sistemes basats en múltiples factora d'autenticació
- Sistemes de clau concertada

☐ Garantir la seguretat i el procés de gestió i custòdia de les claus d'accés:

- Garantir la robustesa de les credencials.
- Implantar mecanismes tècnics de prevenció d'atacs de diccionari o de força bruta.
- Establir un procediment segur de gestió i recuperació de les contrasenyes.
- Garantir que només l'usuari pot conèixer les seves credencials.
- Xifrar les claus.
- Obligar a renovar periòdicament les contrasenyes.

☐ Configurar un *time-out* de sessió i que s'esborri la memòria cau.
☐ Instaurar un registre d'accessos i d'activitat.
☐ Mantenir la informació xifrada (si escau, amb xifratge homomòrfic) sempre que sigui possible.
☐ Emprar signatura electrònica, si és possible.
☐ Assegurar que els processos d'anonimització o pseudonimització emprats no han perdut efectivitat.
☐ Fer proves que comprovin vulnerabilitats a atacs i programar-les de manera periòdica.
☐ Auditar periòdicament el codi.
☐ Establir mecanismes de detecció automàtica d'intrusions i fuites d'informació.
☐ Adoptar qualsevol altra mesura de seguretat adequada als riscos existents.

Disponibilitat

☐ Configurar l'execució de còpies de seguretat.
☐ Establir permisos diferenciats per accedir a les diferents còpies (back-ups).
☐ Preveure proves de recuperació de la informació a partir de còpies.
☐ Valorar redundar el maquinari, subministrament elèctric i xarxes de connectivitat.

Limitació del termini de conservació

☐ Definir el període de conservació de la informació i informar-ne les persones afectades.
☐ Implementar mecanismes automatitzats per facilitar el compliment dels terminis de supressió i bloqueig establerts.
☐ Aplicar mesures com ara l'anonimització si les dades es volen conservar les dades amb finalitats estadístiques més enllà del període de conservació establert.
☐ Destruir els suports de manera efectiva quan es tracti d'elements de maquinari que es deixen d'utilitzar.
☐ Verificar que no s'utilitzen galetes persistents o, alternativament, fixar data de caducitat per aquest tipus de galeta.