# Privadesa en la publicació de dades

PID_00270377

Alexandre Viejo

Temps mínim de dedicació recomanat: 5 hores

Universitat Oberta de Catalunya

**Alexandre Viejo**

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

Primera edició: febrer 2020
© Alexandre Viejo
Tots els drets reservats
© d'aquesta edició, FUOC, 2020
Av. Tibidabo, 39-43, 08035 Barcelona
Realització editorial: FUOC

*Cap part d'aquesta publicació, incloent-hi el disseny general i la coberta, no pot ser copiada, reproduïda, emmagatzemada o transmesa de cap manera ni per cap mitjà, tant si és elèctric com mecànic, òptic, de gravació, de fotocòpia o per altres mètodes, sense l'autorització prèvia per escrit del titular dels drets.*

# Índex

# Introducció

En el context actual de la societat de la informació és generalment senzill trobar informació sobre la nostra identitat, hàbits, interessos o opinions, publicada en fonts electròniques diverses i heterogènies com bases de dades governamentals, plataformes comercials o xarxes socials. Aquesta situació és especialment sensible atès que la quantitat d'informació sobre nosaltres que queda publicada a l'abast de moltes persones tendeix a augmentar amb el temps i roman disponible durant llargs períodes de temps. Com a resultat d'això, les dades que es poden recopilar sobre nosaltres creixen i es tornen més detallades amb el pas del temps.

**Lectura recomanada**

**Sánchez, D.; Viejo, A.** (2017). «Personalized privacy in open data sharing scenarios». *Online Information Review* (vol. 41, núm. 3).

La recol·lecció i explotació de dades personals s'ha convertit en un negoci lucratiu que ha vist florir la indústria dels *data brokers*, entitats que compilen i analitzen la informació dels consumidors per revendre-la o proporcionar serveis comercials. Aquest tipus de negoci va reportar ingressos anuals de més de mil milions de dòlars el 2014.

**Lectura recomanada**

**US Federal Trade Commission** (2014). Data brokers, a call for transparency and accountability.

En paral·lel a l'increment imparable de la publicació de dades personals a la xarxa, la societat en conjunt ha experimentat un augment significatiu de la comprensió de les amenaces a la privadesa que poden produir la recol·lecció i explotació incontrolades d'aquestes dades personals. Aquestes amenaces inclouen accions discriminatòries, explotació no ètica de dades, atacs informàtics de tipus pesca de credencials i, en definitiva, qualsevol activitat lesiva per a la dignitat i els drets dels afectats. Un dels fruits més significatius d'aquesta preocupació global respecte a la privadesa de dades és el Reglament general de protecció de dades (RGPD), regulació europea relativa a la protecció de les persones físiques pel que fa al tractament de les seves dades personals i a la lliure circulació d'aquestes.

**Lectura recomanada**

**Parlamento Europeo** (2016). *Reglamento (UE) 2016/679, general de protección de datos (RGPD)* [en línia]. <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

Cal destacar que el dret a la privadesa no és un concepte nou: el 1890 l'article «The right to privacy» de Warren and Brandeis presentava la privadesa com una part del dret fonamental a la vida. No obstant això, els avenços tecnològics actuals, inclosos els ordinadors, la connectivitat mitjançant internet i el programari capaç de recol·lectar i processar grans quantitats de dades, han posat aquest dret sota el focus convertint-lo en un dret fonamental per si mateix, present en les constitucions de cent cinquanta països.

**Lectura recomanada**

**Warren i Brandeis** (1890). «The right to privacy». *Harvard Law Review* (vol. 193).

Pel que fa a la protecció de les dades de les persones, la legislació sobre privadesa es basa en diversos principis, com limitar la recopilació de dades, especificar el propòsit d'aquesta recol·lecció, limitar l'ús de les dades recol·lectades, proporcionar a l'individu el control sobre la gestió i ús de les seves dades, etc. No obstant això, amb l'auge de la indústria de les dades massives i la seva capacitat per a extreure, analitzar i monetitzar tota peça d'informació present a la xarxa, és clarament dubtós que aquests principis en què es basa la protecció de dades es puguin aplicar de manera efectiva.

**Lectura recomanada**

**Soria-Comas, J.; Domingo-Ferrer, J.** (2015). «Big data privacy: challenges to privacy principles and models». *Data Science and Engineering* (pàg. 1-8).

Entre tots els aspectes relacionats amb la privadesa de la informació, aquesta documentació se centra en la privadesa de la publicació o difusió de dades, un àmbit que ha rebut molta atenció per part de la comunitat científica. En aquest sentit la difusió de dades és la tasca principal dels instituts nacionals d'estadística, els quals pretenen oferir una imatge precisa de la societat; amb aquesta finalitat, recopilen i publiquen dades estadístiques en una àmplia gamma d'aspectes com l'economia, la població, etc. En aquest àmbit la legislació associa generalment la violació de la privadesa amb la identificació d'individus en les dades difoses.

**Lectura recomanada**

**Domingo-Ferrer, J.; Sánchez, D.; Soria-Comas, J.** (2016). *Database anonymization: privacy models, data utility, and microaggregation-based inter-model connections*. Morgan & Claypool Publishers.

# Objectius

En els materials didàctics associats a aquest mòdul l'estudiant trobarà els continguts necessaris per a aconseguir els objectius següents:

**1.** Conèixer els tipus de dades habituals que s'utilitzen en publicar informació en entorns oberts com internet.

**2.** Conèixer els dos objectius principals a l'hora de proporcionar privadesa en la publicació de dades.

**3.** Entendre la diferència entre dades anonimitzades i dades pseudonimitzades.

**4.** Conèixer el problema que cal resoldre per a anonimitzar un conjunt de dades.

**5.** Entendre què és el risc de revelació d'identitat i què és el risc de revelació d'atribut.

**6.** Conèixer els mètodes d'anonimització de dades més habituals.

**7.** Entendre la importància de preservar la utilitat de les dades protegides i conèixer com els diferents mètodes d'anonimització la redueixen.

**8.** Conèixer el model de privadesa *k*-Anonimitat i les seves extensions.

**9.** Conèixer l'anonimització de dades transaccionals, de moviment d'objectes i textuals i entendre les seves diferències respecte a les habituals microdades.

**10.** Entendre els conceptes de protecció de dades des de la privadesa i protecció de dades per defecte.

**11.** Conèixer què són les tecnologies garants de la privacitat i la seva utilitat en la protecció de dades personals.

**12.** Conèixer què són les avaluacions d'impacte en la protecció de dades (AIPD) i la seva utilitat per a complir el principi de protecció de dades des del disseny.

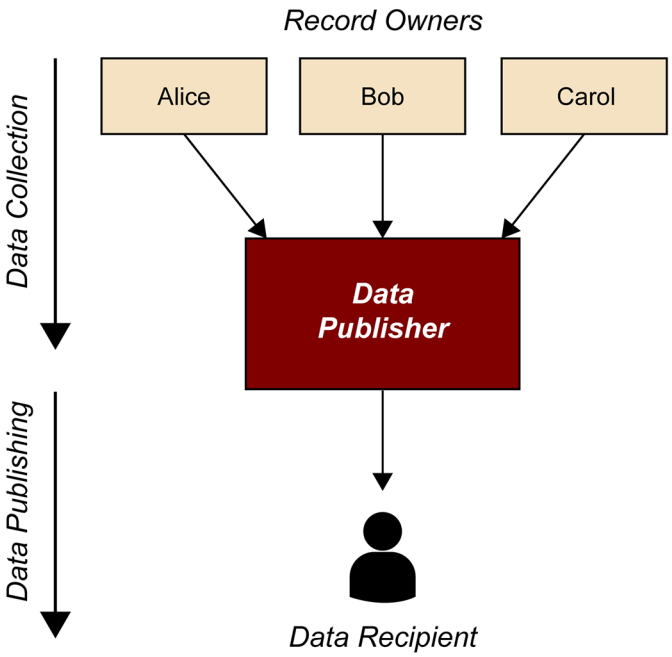
# 1. La publicació de dades personals

La figura 1 descriu l'esquema tipus de recol·lecció i publicació de dades en un entorn obert. En **l'etapa de recol·lecció** *(data collection)* l'entitat publicadora (*data publisher*) recol·lecta les dades dels individus als quals pertanyen (*record owners*). En **l'etapa de publicació** *(data publishing)* l'entitat publicadora difon les dades recol·lectades a terceres persones (*data recipient*), això és, entitats que aplicaran tècniques de mineria de dades sobre aquestes dades per generar nou coneixement, o el públic en general. Un exemple d'aquest escenari és un hospital que recull dades dels seus pacients i publica o proporciona els registres de dades resultants a un centre de recerca extern.

***Record owners***

El terme *propietari de dades* és controvertit i discutible. S'utilitza habitualment en la literatura sobre privadesa en l'àmbit tecnològic. No obstant això, en altres àmbits, com el jurídic, aquest terme és més qüestionable i es parla d'*interessat* o *afectat* en el seu lloc.

Figura 1. Esquema tipus de recol·lecció i publicació de dades




Font: elaboració pròpia (adaptat de Benjamin *et al.*, 2010)

Tal com s'indica a Benjamin, C. M. F.; Ke Wang, R. C.; Philip, S. Y. (2010), hi ha dos models d'entitats publicadores: 1) l'entitat no confiable, que pot intentar identificar dades sensibles en els registres recol·lectats, i 2) l'entitat confiable, que es comporta de manera honesta amb els propietaris de les dades i se cenyeix a recol·lectar i publicar les seves dades. En un escenari en què les dades recol·lectades han de ser protegides abans de publicar-les per a impedir atacs a la privadesa dels individus, l'entitat publicadora de les dades generalment és a càrrec d'aplicar les tècniques necessàries per a proporcionar aquesta protecció. Per aquesta raó, en la literatura s'assumeix habitualment que l'**entitat publicadora és confiable**, la qual cosa també farem en aquesta documentació.

**Lectura recomanada**

**Benjamin, C. M. F.; Ke Wang, R. C.; Philip, S. Yu** (2010). «Privacy-preserving data publishing: a survey of recent developments». *ACM Computing Surveys* (vol. 42, núm. 4, art. 14).

Una altra característica de l'entitat publicadora és que es considera **no experta** en l'ús posterior de les dades recol·lectades i publicades. Això implica que les dades que difon aquesta entitat no es processen per a un ús concret per part dels receptors finals. En lloc d'això, l'entitat publicadora difon un conjunt de registres de dades recol·lectades al més general i útil possible, de manera que aquest conjunt tindrà múltiples aplicacions diferents, utilitzables per diferents tipus de receptors finals.

Respecte a l'entitat receptora de les dades, es considera **no confiable**, això és, assumim que el receptor de les dades sempre intentarà identificar individus en les dades difoses. D'aquesta manera, la protecció aplicada per l'entitat publicadora a les dades recol·lectades té com a funció protegir els propietaris de les dades d'aquestes entitats receptores.

### 1.1. Tipus de dades

La tipologia a la qual pertanyen les dades que es publicaran determina les amenaces potencials a la privadesa que representen i les tècniques de protecció que caldrà aplicar sobre les dades.

Una base de dades representa una col·lecció de dades ben organitzada que permet gestionar-les de manera simple afegint, eliminant, modificant o obtenint la informació emmagatzemada de manera eficient. Les **bases de dades estadístiques** són bases de dades utilitzades amb finalitats d'anàlisi estadística i es consideren el vector de publicació de dades personals més habitual atès que són un element fonamental per a elaborar estudis de tot tipus.

**Lectura recomanada**

**Domingo-Ferrer, J.; Sánchez, D.; Soria-Comas, J.** (2016). *Database anonymization: privacy models, data utility, and microaggregation-based inter-model connections*. Morgan & Claypool Publishers.

Les bases de dades estadístiques es publiquen en dos formats diferents:

- Dades tabulars: dades que han estat agregades sota certes unitats col·lectives i agrupacions. Com a resultat d'això, les referències a individus han estat eliminades de la base de dades. Aquests tipus de dades són les habituals en les bases de dades estadístiques publicades per instituts d'estadística. Per exemple, una taula en una base de dades d'aquest tipus pot ser d'aquesta manera:

Taula 1

| Estat | Salari mitjà (dòlars) |
|---|---|
| Alabama | 39.832 |
| Alaska | 59.902 |

- Microdades: el terme *microdada* es refereix a qualsevol registre que conté informació relativa a un individu especific (ciutadà, empresa, etc.). Les microdades es publiquen sense tractar i poden contenir informació molt detallada sobre les persones o empreses (els *record owners*) a les quals fan

referència les dades emmagatzemades. Seguint l'exemple anterior, un conjunt de registres de microdades podria ser d'aquesta manera:

Taula 2

| Nom | Estat | Salari (dòlars) |
|---|---|---|
| Alice | Alabama | 25.000 |
| Bob | Alaska | 40.500 |
| Carol | Alabama | 51.000 |

Dels dos tipus indicats podem concloure que les dades tabulars, per la seva naturalesa rígida, agregada i lliure de referències a individus, no requereixen aplicar tècniques per a protegir la privadesa de la informació continguda; d'altra banda, les microdades contenen detalls sensibles dels individus i ofereixen el grau de flexibilitat més alt: el *data recipient* pot aplicar qualsevol tipus d'anàlisi sobre aquests detalls atès que les dades es presenten sense cap tipus de tractament ni precàlcul (com l'agregació que hem vist en el cas de les dades tabulars). És per això que la publicació de registres de microdades és la més perillosa per a la privadesa dels individus i ha rebut més atenció per part de la comunitat científica.

### 1.2. Registres de microdades

Com ja hem vist anteriorment, un conjunt de registres de microdades es representa generalment com una taula on cada fila correspon a un individu (*record owner*) i cada columna conté informació respecte a un dels atributs recol·lectat d'aquest individu.

Els atributs d'un registre de microdades es poden classificar segons les categories següents:

- Identificadors: un atribut és un identificador si proporciona una reidentificació inequívoca de l'individu al qual es refereix el registre. Exemples d'atributs identificadors són: número de DNI, número de passaport o número de telèfon mòbil. Si un registre conté un identificador, qualsevol informació confidencial reflectida pels altres atributs pot vincular-se immediatament a un individu específic.
  Per a evitar la reidentificació directa d'un individu per mitjà d'un atribut identificador, aquests s'han d'esborrar dels registres abans de la seva publicació. Una alternativa a l'esborrament és xifrar aquests atributs o substituir-los per un valor que oculti el veritable valor (un pseudònim). Cal destacar que aquesta alternativa, tot i els seus avantatges respecte a l'esborrament, s'ha demostrat insegura per a la privadesa dels *record owners* i es discutirà més endavant.

- Quasi-identificadors: un atribut quasiidentificador no condueix per si mateix i de manera aïllada a reidentificar un individu en els registres. No obstant això, la combinació d'una sèrie d'atributs quasiidentificadors pot permetre reidentificar inequívocament algunes persones. En aquest sentit el treball presentat a Latanya (2000) per Latanya Sweeney va demostrar que el 87% de la població dels Estats Units es pot identificar sense ambigüitats combinant un codi postal de cinc dígits, la data de naixement i el sexe, tots quasiidentificadors aparentment innocus en considerar-se per separat.
  A diferència dels atributs identificadors, en aquest cas esborrar (o xifrar) directament tots els atributs quasiidentificadors no és una opció viable. Això és perquè la majoria de les vegades es requereixen quasiidentificadors per a fer qualsevol anàlisi útil de les dades. Més endavant explicarem els mètodes d'anonimització que es poden aplicar en aquest tipus d'atributs per a protegir la privadesa dels *record owners*.
  Cal destacar que decidir si un cert atribut ha de ser considerat quasiidentificador és un tema complex: si considerem *un atacant que no té coneixement addicional* sobre els individus que cal reidentificar, solament els atributs disponibles en un conjunt de dades extern no anonimitzat(per exemple, una taula amb dades censals) s'han de classificar com a quasiidentificadors. Per contra, en presència d'*atacants ben informats*, qualsevol atribut pot ser potencialment un quasiidentificador o pot no ser-ho, tot dependrà del grau d'informació addicional que tingui l'atacant.

- Confidencials: els atributs confidencials contenen informació confidencial sobre els individus que van participar en el procés de recopilació de dades (*record owners*). Exemples d'informació confidencial són: salari, orientació sexual, estat de salut, etc. L'objectiu principal de les tècniques de protecció de la privadesa és evitar que els atacants puguin rebre informació confidencial sobre un individu específic. Aquest objectiu implica no solament evitar que l'intrús determini el valor exacte que pren un atribut confidencial per a un cert individu, sinó evitar que l'atacant pugui inferir aquest valor de manera més o menys precisa.

- No-confidencials: els atributs no-confidencials són els que no pertanyen a cap de les categories anteriors. Aquest tipus d'atribut no conté informació sensible sobre els individus i no es pot utilitzar per a reidentificar registres. Com a resultat d'això, aquests atributs no afecten de cap manera el procés de protecció de la privadesa aplicat a la publicació de dades i no seran considerats en aquest document.

A continuació mostrem una taula d'exemple amb registres de microdades respecte als pacients d'un hospital i les malalties que els han estat diagnosticades. En aquesta taula podem veure els tres tipus d'atributs considerats: identificadors, quasiidentificadors i confidencials.

**Lectura recomanada**

**Latanya, S.** (2000). «Uniqueness of simple demographics in the U.S. population». *LIDAP-WP4*. Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh PA.

Taula 3

| DNI | Codi postal | Edat | Sexe | Malaltia |
|---|---|---|---|---|
| 37713522Z | 08017 | 37 | Home | Hepatitis |
| 41343621B | 08242 | 25 | Home | Hepatitis |
| 36689764P | 43005 | 45 | Dona | HIV |
| 74452667A | 08040 | 49 | Home | Grip |

El camp DNI és l'atribut identificador que hauria de ser esborrat com a primer pas en un procés d'anonimització de les dades. Els camps codi postal, edat i sexe són atributs quasiidentificadors, els quals, combinats, poden arribar a reidentificar un pacient. Finalment, el camp malaltia és l'atribut confidencial, que un atacant en cap cas no hauria de poder vincular a l'individu corresponent.

# 2. Privadesa en la publicació de dades: anonimat i confidencialitat

Fins ara hem parlat de registres de microdades i de protegir la privadesa dels *record owners* que han generat aquestes microdades. Quan parlem de protegir la privadesa hem de tenir en compte que en la literatura aquesta protecció es fa partint de dos objectius de privadesa diferents:

- **Obtenir confidencialitat** (en anglès, *confidentiality*): accedir al conjunt de dades publicat no hauria de revelar informació confidencial vinculada a cap individu específic.

- **Obtenir anonimat** (en anglès, *anonymity*): no hauria de ser possible reidentificar cap individu en el conjunt de dades publicat.

Protegir dades per obtenir confidencialitat busca limitar la quantitat d'informació que un conjunt de registres de microdades proporciona al *data recipient*. Una manera habitual d'aconseguir això és emmascarar els valors confidencials afegint soroll. Per exemple, si sumem o restem números aleatoris dins d'un cert rang, per exemple, entre 5 i 10 (això seria el «soroll»), al camp edat d'una taula de microdades, el *data recipient* obtindrà les edats dels individus amb una distorsió d'entre 5 i 10 punts, la qual cosa no li permetrà conèixer les edats exactes dels *record owners*. La quantitat de soroll afegida determina directament el nivell de confidencialitat obtingut. D'aquesta manera, seguint amb l'exemple, si afegim molt poc soroll (valors entre 1 i 3), el *data recipent*, encara que no obtingués el valor exacte, sí que obtindria un valor molt semblat al real; d'altra banda, si afegim molt soroll (valors entre 10 i 20), el *data recipient* obtindria un valor tan allunyat del valor real que caldria valorar si aquest ha deixat de ser útil. En aquest sentit més endavant parlarem sobre l'equilibri entre la protecció de la privadesa i la utilitat de les dades protegides.

D'altra banda, protegir dades per obtenir anonimat busca ocultar cada individu (cada *record owner*) en un grup d'individus «similars», de manera que no sigui possible identificar un individu concret dins d'aquest grup (una idea relacionada amb l'«anonimat de la multitud»). Aquest objectiu és aplicat típicament per la comunitat científica per desenvolupar els seus models de privadesa, que al seu torn són essencials per a oferir garanties de privadesa en protegir conjunts de dades. Un exemple de model de privadesa basat en aquest objectiu és la cèlebre k-Anonimitat (en anglès, *k-anonymity*), model del qual parlarem amb detalls més endavant.

**Lectura recomanada**

**Samarati, P.; Latanya, S.** (1998). «Protecting privacy when disclosing information: *k*-anonymity and its enforcement through generalization and suppression». *Technical report* . SRI International.

## 2.1. Dades anonimitzades i dades pseudonimitzades

Tal com hem dit, un procés basat en *anonimitzar dades* busca evitar la reidentificació d'individus en les dades anonimitzades. D'aquesta manera, el primer pas en qualsevol procés d'anonimització és eliminar els atributs identificadors dels registres que cal protegir; els passos següents es basaran a alterar, seguint certes tècniques, la resta dels atributs presents en les dades. Com a resultat d'aquest procés, obtindrem unes dades anonimitzades, en les quals **s'ha trencat tot vincle entre els individus que van generar les dades (*record owners*) i les dades resultants protegides**. Cal destacar que eliminar el vincle entre individus i les seves dades implica destruir informació inherent a aquestes dades, la qual cosa repercuteix al seu torn en la utilitat que es pot extreure de les dades protegides (unes dades que proporcionen menys informació seran forçosament menys útils per a un *data recipient*).

En explicar els atributs identificadors vam indicar que una alternativa a eliminar-los era xifrar-los o substituir-los per altres valors que ocultessin l'identificador real. En tots dos casos el que fem és substituir l'atribut identificador d'un individu per un pseudònim. Aquesta és la base de les *dades pseudonimitzades*. Els dos avantatges principals respecte a les dades anonimitzades són: 1) **els pseudònims oculten la identitat però mantenen el vincle entre les dades** (les dades protegides retenen més informació, així que són més útils), i 2) l'entitat que ha generat els pseudònims (sigui mitjançant xifratge o per simple substitució de valors) és capaç de revertir el procés de pseudonimització i recuperar les dades originals en cas de ser necessari.

**Lectura recomanada**

**Barbaro M.; Zeller T.** (2006). «A face is exposed for AOL searcher no. 4417749». *New York Times* (agost).

Per posar un exemple representatiu de les dues formes de protecció, podem assumir la base de dades d'un motor de cerca web (com Google), on aquesta entitat emmagatzema totes les consultes que els usuaris envien (aquestes bases de dades es coneixen com a *query logs*). La primera taula correspon a cinc consultes reals extretes dels *query logs* publicats per l'empresa AOL l'any 2006. Aquests *query logs* eren formats per vint milions de consultes fetes per 657.426 usuaris. Per a protegir-los, AOL va substituir els atributs identificadors dels usuaris per pseudònims en forma de nombre:

Taula 4

| Pseudònim | Consulta | Data | URL seleccionada |
|---|---|---|---|
| 2178 | *Dog cornea treatment* | 2006-03-27 | <http://www.2ndchance.info> |
| 2178 | *Pergola house entrance* | 2006-04-08 | <http://www.gardenstructure.com> |
| 2178 | *Pennsylvania college savings* | 2006-03-16 | <http://www.patreasury.org> |
| 2178 | *Inducing dog vomiting* | 2006-05-26 | <http://dogs.about.com> |
| 1326 | *Holiday mansion house boat* | 2006-04-06 | <http://www.iboats.com> |

Un observador extern que tingui accés a aquesta taula, no pot conèixer *a priori* la identitat de l'individu darrere del pseudònim «2178», però sí que pot fer un perfil més o menys precís dels interessos, problemes, lloc de residència, etc. de l'individu que s'oculta darrere del pseudònim. Això pot permetre a l'observador saber quines pàgines web acostuma a consultar una persona amb aquests interessos, i potser pugui servir per a fer algun estudi de màrqueting o similar. Aquesta taula basada en dades pseudonimitzades és capaç de proporcionar aquest coneixement perquè manté el vincle entre les dades i l'individu que les ha generat, tot i que se n'oculti la identitat.

En contrast, eliminar directament els atributs identificadors ens proporcionaria una taula anonimitzada com aquesta:

Taula 5

| Consulta | Data | URL seleccionada |
|---|---|---|
| *Dog cornea treatment* | 2006-03-27 | <http://www.2ndchance.info> |
| *Pergola house entrance* | 2006-04-08 | <http://www.gardenstructure.com> |
| *Pennsylvania college savings* | 2006-03-16 | <http://www.patreasury.org> |
| *Inducing dog vomiting* | 2006-05-26 | <http://dogs.about.com> |
| *Holiday mansion house boat* | 2006-04-06 | <http://www.iboats.com> |

En aquesta taula un observador extern no pot vincular de cap manera les consultes que hi apareixen. Des del seu punt de vista, cada consulta és independent de les anteriors i no pot inferir un perfil d'interessos d'un individu en concret.

Des del punt de vista de preservar la utilitat de les dades, pseudonimitzar en lloc d'anonimitzar representa un clar avantatge. No obstant això, s'ha demostrat que una protecció basada en pseudonimitzar és feble i, de fet, no és un mètode de protecció de dades acceptat per la comunitat científica. En particular, seguint amb la publicació massiva de dades que va fer AOL, en aquest cas els periodistes del *New York Times* Michael Barbaro i Tom Zeller expliquen en el seu article amb quina facilitat van ser capaços de rastrejar un pseudònim fins a la seva identitat real associada. En particular, els dos periodistes van ser capaços d'associar el número «4417749» amb la persona anomenada Thelma Arnold, la qual havia fet consultes com: «homes solters de 60», «gos que es pixa per tot arreu», «paisatges a Lilburn» i nombroses consultes relacionades amb el cognom «Arnold». Després de l'escàndol, AOL va eliminar l'accés al *query log* publicat; no obstant això, avui dia encara circulen còpies d'aquests registres.

**Lectura recomanada**

**Barbaro M.; Zeller T.** (2006). «A face is exposed for AOL searcher no. 4417749». *New York Times* (agost).

A causa de la feblesa de l'ús de pseudònims, la literatura sobre privadesa se centra generalment en l'anonimització de dades, ja que el seu objectiu és la dissociació total de les dades i és, per tant, la metodologia més segura des del punt de vista de la privadesa. En conseqüència, en aquesta documentació

també ens centrarem en l'anonimització de dades i els mètodes existents per a aconseguir-la. No obstant això, cal destacar que, a la pràctica, aconseguir una anonimització perfecta, entenent com tal una dissociació de les dades irreversible i total, és una tasca d'una dificultat molt elevada. A més, no és possible proporcionar garanties que un conjunt de dades anonimitzades romandrà protegit indefinidament, atès que la reidentificació per part d'un atacant depèn en gran manera de la informació externa que tingui, i la possibilitat que un atacant obtingui nova informació addicional en el futur que trenqui l'anonimització feta a data d'avui està fora del control de l'entitat encarregada de protegir les dades.

La impossibilitat pràctica de fer una anonimització perfecta (més enllà de distorsionar o eliminar simplement les dades protegides fins a arribar al punt que la utilitat de les dades resultants sigui zero) té certes implicacions a l'hora de protegir dades aplicant la legislació.

En concret, segons s'indica en *La k-Anonimidad como medida de la privacidad* (2019), la Directiva 95/46 en el considerant 26 establia que, per a determinar si una persona era identificable, era necessari considerar el conjunt dels mitjans que podien ser utilitzats raonablement pel responsable del tractament o per qualsevol altre, per a identificar aquesta persona. D'aquesta manera, deixaven de ser aplicables els principis de protecció de dades en els casos en què el conjunt de dades s'hi havia anonimitzat de manera tal que ja no era possible identificar l'interessat. En la mateixa línia, el considerant 26 del RGPD assenyala que les dades pseudonimitzades constitueixen informació sobre una persona física a partir de la qual és possible fer-ne la identificació amb una probabilitat raonable, tenint en compte mitjans i factors objectius i els costos, temps i tecnologia necessaris per a materialitzar-ne la identificació.

**Lectura recomanada**

**Agencia Española de Protección de Datos** (2019). *La k-Anonimidad como medida de la privacidad* [en línia]. <https://www.aepd.es/media/notas-tecnicas/nota-tecnica-kanonimidad.pdf>

La primera implicació d'aquesta situació és que no és rar trobar documentació en la qual s'igualen els conceptes pseudonimització i anonimització, atès que el fet que l'anonimització no sigui perfecta obre la porta al fet que sigui un procés reversible, a semblança de la pseudonimització. La segona implicació és que les dades anonimitzades (com les pseudonimitzades) quedarien emparades per l'àmbit d'aplicació de les normes sobre protecció de dades (sempre que hi hagi aquesta probabilitat de reidentificació), donada la probabilitat raonable que la seva protecció sigui reversible i la reidentificació d'individus possible.

### 2.2. El problema a resoldre per a anonimitzar dades

Anteriorment hem argumentat l'aplicació de l'anonimització de dades (amb les seves imperfeccions) per part dels experts en l'àrea a l'hora de protegir informació que serà publicada en entorns oberts. En aquest apartat formalitza-

rem el problema que aquests experts han de resoldre cada vegada que han d'anonimitzar un cert conjunt de dades. Això és el que es coneix com a problema de l'anonimització (en anglès, *anonymization problem*).

El **problema de l'anonimització** és produir una taula anonimitzada a partir d'una taula original, que satisfaci uns certs requeriments de privadesa, determinats pel model de privadesa seleccionat i que retingui la major quantitat d'informació (utilitat) possible.

Més endavant detallarem les operacions que s'utilitzen per a anonimitzar un conjunt de dades, introduirem els models de privadesa que se solen aplicar i explicarem l'equilibri requerit entre la necessitat d'obtenir informació de la taula protegida amb una determinada fidelitat i el cost que el procés d'anonimització pot tenir per a la privadesa dels individus.

# 3. Riscos de revelació d'informació confidencial

Quan es publiquen registres de microdades, l'entitat publicadora (*data publisher*) ha d'evitar que es divulgui informació sensible o confidencial dels individus (*record owners*) dels quals s'ha obtingut les dades. Generalment, es consideren dos tipus de riscos de revelació:

- Revelació de la identitat (en anglès, *identity disclosure*): aquest risc s'aplica directament a la privadesa vista com l'obtenció de l'anonimat i té lloc quan l'atacant reidentifica un individu en el conjunt de dades publicat i protegit; això és, l'atacant és capaç de vincular un registre d'aquest conjunt de dades amb l'individu que el va originar. Una vegada l'atacant ha reidentificat un individu, pot associar els valors dels atributs confidencials a aquesta persona.

  Per a mesurar el risc de revelació de la identitat, el *data publisher* aplica generalment un mètode de vinculació entre registres (en anglès, *record linkage*) sobre les dades protegides abans de publicar-les. Hi ha diversos algorismes de *record linkage* en la literatura, però la idea bàsica és buscar la similitud entre els registres protegits i els registres originals per calcular el percentatge de «parelles» detectades. Detectar una parella de registres implica que el registre original i el registre anonimitzat són massa semblants i, per tant, un atacant podria aconseguir una reidentificació. Si el percentatge de parelles detectat és elevat, el *data publisher* hauria de tornar a anonimitzar les dades fins a aconseguir un nivell de risc raonable de revelació de la identitat.

  Com s'ha dit, hi ha diferents algorismes de *record linkage*. El més senzill es basa a buscar valors d'atributs coincidents entre la taula original i la taula protegida; per exemple, podríem buscar la combinació dels tres atributs quasiidentificadors més cèlebres (codi postal, data de naixement i sexe en ambdues taules) i detectar les coincidències:

**Lectura recomanada**

Sobre els dos tipus de riscos de revelació:

**Hundepool, A.; Domingo-Ferrer, J.; Franconi, L. *et al.*** (2012). *Statistical disclosure control*. Wiley.

Taula 6. Taula original

| DNI | Codi postal | Edat | Sexe | Malaltia |
|---|---|---|---|---|
| 37713522Z | 08017 | 37 | Home | Hepatitis |
| 36689764P | 43005 | 45 | Dona | HIV |

Taula 7. Taula protegida

| DNI | Codi postal | Edat | Sexe | Malaltia |
|---|---|---|---|---|
| * | 08017 | 37 | Home | Hepatitis |
| * | * | * | Dona | HIV |

En aquest cas l'algorisme detectaria en la taula protegida el registre corresponent a l'usuari amb DNI 37713522Z, atès que els tres quasiidentificadors coincideixen. D'altra banda, l'usuari amb DNI 36689764P no seria detectat en la taula protegida.

- Revelació de l'atribut (en anglès, *attribute disclosure*): aquest risc s'aplica directament a la privadesa vista com a obtenció de la confidencialitat i té lloc quan l'atacant és capaç de determinar amb prou precisió el valor d'un atribut confidencial a partir del conjunt de dades publicat i protegit.

Tal com s'indica a Domingo-Ferrer *et al.* (2016), els dos tipus de risc de revelació considerats són independents. Això implica que si un atacant és capaç de reidentificar un individu en les dades publicades això no garantiria que l'atacant acabés coneixent l'atribut confidencial (o atributs confidencials) associats a aquest registre, atès que aquests es podrien haver emmascarat afegint soroll; per tant, en aquest cas concret hi hauria revelació de la identitat però no revelació de l'atribut

**Lectura recomanada**

**Domingo-Ferrer, J.; Sánchez, D.; Soria-Comas, J.** (2016). *Database anonymization: privacy models, data utility, and microaggregation-based inter-model connections*. Morgan & Claypool Publishers.

D'altra banda, la revelació d'atribut pot tenir lloc fins i tot sense que hi hagi revelació de la identitat. Per exemple, suposant una taula que conté els treballadors d'una empresa en la qual el salari és un atribut confidencial i el lloc de treball un quasiidentificador, si un atacant vol conèixer el salari d'un cert treballador i sap que el seu lloc de treball és «administratiu», encara que no pugui reidentificar el treballador amb el seu registre en la taula, sabent solament que és un «administratiu» (atès que hi haurà molts «administratius» en la taula) sí que podrà conèixer el rang de salari en què està aquest treballador, atès que podrà conèixer tots els salaris de tots els treballadors; si el rang de possibles valors salarials per a «administratius» és prou estret, tindrà lloc la revelació de l'atribut.

# 4. Mètodes d'anonimització per microdades

Per a evitar els riscos de revelació d'identitat o atribut, els *data publishers* no publiquen les dades recol·lectades originals sinó una versió anonimitzada (o protegida). Per a aquesta tasca, els *data publishers* utilitzen una sèrie de mètodes d'anonimització basats tant a emmascarar les dades originals com a substituir-les per dades sintètiques. En els subapartats següents classificarem i explicarem els mètodes d'anonimització més habituals. Cal destacar que aquests mètodes, a més de ser eines d'anonimització de dades, també són mètodes bàsics per a satisfer els requeriments de privadesa determinats pels diversos models de privadesa que veurem més endavant.

## 4.1. Mètodes d'emmascarament sense pertorbació de dades

Els mètodes d'emmascarament no-pertorbatius no alteren les dades originals; en lloc d'això, les suprimeixen o en redueixen el nivell de detall. En aquesta categoria podem destacar quatre mètodes:

- Generalització (en anglès, *generalization*): aquest mètode, també conegut en la literatura com a *global recoding*, substitueix els valors originals dels atributs per valors més generals; d'aquesta manera es redueix el nivell de detall de les dades originals i, per tant, la quantitat d'informació que proporcionen. Per a emmascarar un atribut seguint aquesta tècnica, és necessari representar tots els valors que l'atribut pot tenir seguint una jerarquia de generalització. En aquesta jerarquia el valor més general estarà situat en el cim, mentre que els valors més específics estaran situats en la base. El procés de generalització treballa substituint els valors específics de les dades originals per valors més generals situats en cotes més altes de la jerarquia, que seran els que apareixeran en el conjunt de dades protegit.
  Per exemple, en cas d'un atribut categòric (els valors d'una variable categòrica són categories o grups mútuament excloents i no admeten operacions aritmètiques) que indica el lloc de treball d'un individu, els valors «professor ajudant doctor» i «professor contractat doctor» es podrien substituir pel valor «professor», més general que els anteriors i que, per tant, els engloba. En cas d'un atribut numèric (valors que admeten operacions aritmètiques) que indica el salari d'un individu, els valors originals es podrien substituir per intervals numèrics.

**Lectura recomanada**

Sobre el *global recoding*:
**Samarati, P.; Latanya, S.** (1998). «Protecting privacy when disclosing information: *k*-anonymityand its enforcement through generalization and suppression». *Technical report*. SRI International.

Taula 8. Taula original

| DNI | Lloc de treball | Salari |
|---|---|---|
| 37713522Z | Professor contractat doctor | 38.000 |
| 36689764P | Professor ajudant doctor | 27.000 |

Taula 9. Taula protegida

| DNI | Lloc de treball | Salari |
|---|---|---|
| * | Professor | 35.000-40.000 |
| * | Professor | 25.000-30.000 |

- *Top and bottom coding*: aquest mètode és un cas especial de generalització en què els valors extrems, que se situen per sobre d'un determinat llindar superior i per sota d'un determinat llindar inferior, són substituïts per un valor únic que representa el valor màxim possible (*top-code*) o el valor mínim possible (*bottom-code*) respectivament. La idea que hi ha darrere d'aquest mètode és que els valors extrems són rars i, per tant, poden facilitar la reidentificació dels individus als quals estan vinculats. Seguint amb l'exemple anterior de la taula de treballadors, és rar trobar treballadors amb edats molt avançades en una empresa. Si l'empresa té un únic treballador de 72 anys, per exemple, de res no servirà emmascarar aquesta edat en una franja del tipus 70-75 anys amb el mètode de generalització, atès que solament aquest treballador estarà en aquesta franja i serà fàcilment reidentificable en la taula protegida. En lloc d'això, s'aplicaria *top coding* i se substituiria l'edat pel valor «>60», per sota del qual s'engloben molts més treballadors de l'empresa. Aquest mètode solament es pot aplicar per definició en atributs que poden ser ordenats de major a menor, com l'edat o el salari.

  En les tres taules següents considerem l'atribut salari com a confidencial i, a més, no li apliquem cap emmascarament (podríem tenir risc de revelació d'atribut tot i evitar la revelació d'identitat). L'atacant vol saber el sou d'un individu i sap que aquest té més de 70 anys. La taula mal protegida no protegeix l'individu 76533777B: solament ell és en la franja d'edat 70-75 i, per tant, l'atacant reidentifica el registre amb aquest individu (tenim revelació d'identitat) i en descobreix el salari (tenim revelació d'atribut). Per contra, en la taula protegida l'atacant es troba tres registres que podrien correspondre amb l'individu; d'aquesta manera, no pot reidentificar-lo i solament pot saber que el seu sou està entre 38.000 i 58.000. Si haguéssim emmascarat el sou, l'atacant encara hauria aconseguit menys informació.

Taula 10. Taula original

| DNI | Edat | Salari |
|---|---|---|
| 37713522Z | 26 | 35.000 |
| 36689764P | 29 | 41.000 |
| 56564576X | 62 | 44.000 |
| 15434434V | 61 | 38.000 |
| 76533777B | 72 | 58.000 |

Taula 11. Taula mal protegida

| DNI | Edat | Salari |
|---|---|---|
| * | 25-30 | 35.000 |
| * | 25-30 | 41.000 |
| * | 60-65 | 44.000 |
| * | 60-65 | 38.000 |
| * | **70-75** | **58.000** |

Taula 12. Taula protegida

| DNI | Edat | Salari |
|---|---|---|
| * | 25-30 | 35.000 |
| * | 25-30 | 41.000 |
| * | >60 | 44.000 |
| * | >60 | 38.000 |
| * | >60 | 58.000 |

- Eliminació (en anglès, *local supression*): aquest mètode es basa simplement a eliminar certs valors dels atributs que es creu que poden facilitar la reidentificació dels *record owners*. És la tècnica que apliquem per eliminar els valors dels atributs identificadors (el primer pas en qualsevol procés d'anonimització). Addicionalment, aquesta tècnica també s'utilitza amb valors d'atributs quasiidentificadors l'existència dels quals resulta en una combinació única en la taula i que, per tant, portarà a una reidentificació. Per exemple, en el cas anterior podríem haver eliminat l'edat de la persona 76533777B en lloc de substituir-la pel *top-code* (cal destacar que en aquest cas tenir un únic registre amb l'edat esborrada podria comportar un problema de privadesa també). Finalment, aquesta tècnica també es pot utilitzar per a esborrar registres sencers directament (la qual cosa solucionaria el problema anterior respecte a la persona 76533777B). No obstant això, és molt important tenir en compte que aplicar aquesta tècnica implica esborrar dades, i cada vegada que s'esborren dades la taula protegida resultant perd informació i, per tant, utilitat. La pèrdua d'utilitat afecta directament l'anonimització, que ens porta al fet que el conjunt de dades protegit reté la major quantitat d'informació (utilitat) possible.

- *Sampling*: aquesta tècnica té alguna relació amb l'anterior en el sentit que es basa a triar un conjunt de registres del conjunt de dades original i publicar-los directament sense cap emmascarament addicional (més enllà d'eliminar els atributs identificadors). Per exemple, podríem publicar solament els registres imparells del conjunt de dades original i eliminar els parells. La protecció que ofereix se sustenta en la incertesa respecte a si el registre d'un cert individu està entre les dades publicades o no. De manera

**Lectura recomanada**

Sobre el mostratge:

**Willenborg, L.; De Waal, T.** (2001). *Elements of statistical disclosure control*. Nova York: Springer-Verlag.

similar al mètode anterior, el fet d'eliminar registres afecta directament la utilitat de les dades protegides.

### 4.2. Mètodes d'emmascarament amb pertorbació de dades

Aquest tipus de mètodes es basa a distorsionar les dades originals per generar el conjunt de dades protegides. Tal com hem indicat anteriorment, els mètodes no-pertorbatius redueixen el detall de les dades originals o les eliminen totalment, però tenim la garantia que totes les dades que apareixen en el conjunt de dades protegides són legítimes. En el cas dels mètodes basats en pertorbació, la distorsió afegida genera unes dades noves vinculades a cada individu que són diferents de les originals. Dins d'aquesta categoria podem destacar tres mètodes:

- Afegir soroll (en anglès, *noise addition*): aquest mètode s'usa habitualment per a emmascarar atributs numèrics considerats confidencials (per exemple, el salari d'una persona). La idea general és substituir el valor original *v* per un valor nou *v+r*, on *r* és un valor aleatori (el soroll que volem afegir) obtingut d'alguna distribució de probabilitat. Segons la distribució de probabilitat que triem per generar el soroll, obtindrem valors aleatoris més o menys alts i amb més o menys freqüència, i, així, uns valors protegits més o menys distorsionats respecte als originals. Com a resultat d'afegir soroll a les dades originals, les dades protegides resultants seran diferents de les legítimes, la qual cosa pot tenir efectes negatius respecte a la utilitat de les dades; no obstant això, depenent del tipus de soroll afegit, les dades protegides, encara que siguin diferents dels originals, seran capaces de preservar informació estadística com la mitjana o la variància de les dades legítimes.

**Lectura recomanada**

Sobre *noise addition*: **Hundepool, A.; Domingo-Ferrer, J.; Franconi, L. *et al.*** (2012). *Statistical disclosure control*. Wiley.

- Intercanvi de dades (en anglès, *data swapping*): la idea general d'aquesta tècnica és anonimitzar una taula de registres mitjançant l'intercanvi dels valors de l'atribut seleccionat entre els registres individuals. D'aquesta manera, els valors originals es mantenen, encara que en el conjunt de dades protegit aquestes apareixen vinculades a altres individus. Aquest mètode manté la informació estadística de la taula protegida, atès que les dades són les mateixos que en la taula original (calcular la mitjana de salaris seria exactament el mateix en la taula original que en la taula protegida); no obstant això, l'intercanvi de vinculació entre individus i valors comporta una pèrdua d'informació rellevant i el fet que sigui un intercanvi aleatori pot donar lloc a vinculacions poc consistents (per exemple, salaris que no concorden amb llocs de treball). Per a mitigar aquest problema de consistència entre valors, hi ha una variació d'aquest mètode anomenada *rank swapping*, en la qual primer s'ordenen els valors que seran intercanviats i els intercanvis es produeixen entre valors propers per aquest ordre; d'aquesta manera, seguint amb l'exemple anterior, el salari d'una persona en un cert lloc de treball s'intercanviaria pel salari d'una altra persona dins

**Lectura recomanada**

Sobre el *data swapping*:
**Dalenius, T.; Reiss, S. P.** (1978). *Data-swapping: a technique for disclosure control, proceedings of the ASA section on survey research methods* (pàg. 191-194).

**Sobre el *rank swapping*:**

**Greenberg, B.** (1996). *Rank swapping for masking ordinal microdata*. Washington DC: U.S. Bureau of the Census.

d'un mateix rang de salaris i, per tant, el sou protegit assignat a l'individu, malgrat no sigui igual a l'original, sí que seria semblant.

- Microagregació (en anglès, *microaggregation*): aquest mètode es basa a substituir els valors originals d'un atribut per un valor agregat que oculti els valors originals però que sigui prou semblat a ells per a preservar-ne la utilitat. El procés d'emmascarament té dues etapes: 1) el conjunt de dades original es parteix en grups de *K* registres intentant que els valors de l'atribut que cal emmascarar dels *K* registres siguin al més similars possibles, i 2) per a cada grup de registres, els valors de l'atribut a emmascarar se substitueixen per un valor representatiu del grup. Aquest valor representatiu serà típicament la mitjana de tots els valors originals; d'aquesta manera, com més homogeni sigui el grup de *K* registres construït en el primer pas, més fidedigne serà el valor representatiu obtingut en aquest segon pas.

**Lectura recomanada**

Sobre la microagregació:
**Defays, D.; Anwar, M. N.** (1998). «Masking microdata using micro-aggregation». *Journal of Official Statistics* (vol. 14, núm. 4, pàg. 449-461).

Taula 13. Taula original

| DNI | Edat | Salari |
|---|---|---|
| 37713522Z | 26 | 35.000 |
| 36689764P | 29 | 41.000 |
| 67457676C | 65 | 61.000 |
| 56564576X | 62 | 44.000 |
| 15434434V | 61 | 38.000 |
| 76533777B | 72 | 68.000 |

Taula 14. Taula protegida (*K* = 2)

| DNI | Edat | Salari | |
|---|---|---|---|
| * | 26 | 36.500 | (35.000 + 38.000) / 2 = 36.500 |
| * | 61 | 36.500 | (35.000 + 38.000) / 2 = 36.500 |
| * | 29 | 42.500 | (41.000 + 44.000) / 2 = 42.500 |
| * | 62 | 42.500 | (41.000 + 44.000) / 2 = 42.500 |
| * | 65 | 64.500 | (61.000 + 68.000) / 2 = 64.500 |
| * | 72 | 64.500 | (61.000 + 68.000) / 2 = 64.500 |

Quan es volen emmascarar molts atributs aquesta tècnica es pot aplicar de manera iterativa per a cada atribut prenent simplement com a entrada la taula protegida resultant de la iteració anterior; aquesta manera de treballar es denomina *univariate* i produeix una baixa pèrdua d'utilitat en les dades protegides a canvi d'un risc significatiu de revelació. Una altra opció és protegir tots els atributs alhora amb el mètode anomenat *multivariate*; en aquest cas, la pèrdua d'utilitat serà molt elevada, però el risc de revelació serà baix.

### 4.3. Generació de dades sintètiques

Aquest tipus de mètodes es basa a eliminar totes les dades originals i substituir-les completament per dades noves generades de manera aleatòria. D'aquesta manera, s'espera protegir la privadesa dels *record owners*, atès que cap dada real seva no apareix realment en les dades protegides. No obstant això, el problema que es presenta en aquests mètodes és aconseguir unes dades aleatòries que dins de la seva aleatorietat retinguin prou informació real perquè les dades protegides resultants tinguin algun tipus d'utilitat.

**Lectura recomanada**

**Rubin, D. B.** (1993). «Discussion: statistical disclosure limitation». *Journal of Official Statistics* (vol. 9, pàg. 462-468).

Per a aconseguir retenir certa informació en les dades protegides, aquests mètodes busquen, primer, crear un model de dades (això és, una seqüència finita de valors possibles) del qual es pugui obtenir de manera aleatòria valors similars als valors originals que volem «simular». Una vegada tinguem aquest model de dades, simplement substituirem els valors originals pels valors que obtinguem de manera aleatòria d'aquest model. Com que se suposa que totes les dades possibles d'aquest model són «semblats» a les originals, s'espera que les dades protegides resultants tindran prou similitud amb les originals per a retenir certa informació estadística; per exemple, podem calcular la mitjana dels valors i s'espera que el resultat no difereixi massa de la mitjana que calcularíem amb els valors originals.

La literatura sobre privadesa considera que aquests mètodes solament tenen valor teòricament, atès que a la pràctica és complicat trobar models de dades que serveixin per a simular de manera fidedigna els valors de qualsevol tipus d'atribut que vulgui ser protegit. A més, com que les dades protegides són sintètiques (això és, falses), l'objectiu principal d'aquests mètodes és publicar un conjunt de dades protegit que retingui certa informació estadística (mitjana, mediana, variància, etc.). Essent aquest l'objectiu principal, ens podríem preguntar si no seria més segur i eficient publicar simplement la informació estadística que volem retenir calculada directament de les dades originals i evitar tot el procés de generació de dades falses aleatòries que intenten retenir aquesta informació estadística.

**Lectura recomanada**

**Domingo-Ferrer, J.; Sánchez, D.; Soria-Comas, J.** (2016). *Database anonymization: privacy models, data utility, and microaggregation-based inter-model connections*. Morgan & Claypool Publishers.

### 4.4. Valoració general dels mètodes d'anonimització presentats

En aquest apartat s'han explicat una sèrie de mètodes d'anonimització de dades i, en general, no és possible presentar-ne un com el més útil o l'únic necessari. Cada mètode podrà ser útil en un cert àmbit d'actuació. No obstant això, d'entre tots sí que podem destacar els mètodes de generalització i eliminació pertanyents a la categoria d'emmascarament no-pertorbatiu. Aquests dos mètodes són sens dubte els més utilitzats per a la tasca de protegir les dades tant en l'àmbit acadèmic com en la indústria. Per això aquests mètodes són els que utilitzarem preferentment en els apartats següents per a explicar com s'apliquen els diversos models de privadesa per a poder satisfer els requeriments de privadesa i resoldre el problema de l'anonimització.

Les raons que trobem per a l'èxit d'aquests dos mètodes són les següents: 1) són molt intuïtius, amb la qual cosa és fàcil entendre com funcionen i el resultat que obtindrem en aplicar-los; 2) ofereixen facilitat en la seva utilització i integració en qualsevol sistema de protecció de dades, i 3) generen dades protegides totalment legítimes en contrast amb altres solucions que generen dades falses, la qual cosa ajuda a retenir la utilitat de les dades anonimitzades.

# 5. Preservació de la utilitat de les dades anonimitzades

Tal com s'indica a Rodríguez (2017), limitar els riscos de revelació en les dades que cal publicar implica modificar d'alguna manera les dades originals. Aquestes modificacions causen una pèrdua d'informació en les dades protegides i aquestes perden al seu torn utilitat per als *data recipients* que volen analitzar-les i extreure'n coneixement. En qualsevol cas, la mesura real d'utilitat que proporcionen unes dades protegides depèn directament de l'ús posterior que se'n farà: un conjunt de dades protegides pot ser útil per a certs tipus d'anàlisis però totalment inútil per a unes altres. La gran varietat d'usos potencials de les dades fa que sigui generalment impossible per al *data publisher* saber, a l'hora d'anonimitzar unes dades, per a què s'usaran posteriorment aquestes dades protegides, la qual cosa comporta un problema important que impedeix ajustar correctament la balança entre utilitat de les dades i protecció de la privadesa. Com que les dades es protegeixen generalment sense tenir en compte l'ús posterior que se'ls donarà, en la literatura es considera més apropiat parlar de **pèrdua d'informació** en lloc d'utilitat.

**Lectura recomanada**

Sobre la pèrdua d'informació:
**Domingo-Ferrer, J.; Sánchez, D.; Soria-Comas, J.** (2016). *Database anonymization: privacy models, data utility, and microaggregation-based inter-model connections*. Morgan & Claypool Publishers.

**Lectura recomanada**

**Rodríguez, M.** (2017). *Semantic perturbative privacy-preserving methods for nominal data*. Tesi doctoral. Universitat Rovira i Virgili.

Per a minimitzar la pèrdua d'informació d'un conjunt de dades protegides, l'estratègia més habitual és maximitzar la preservació de l'estructura analítica de les dades originals. Exemples dels elements que seria desitjable preservar són: la mitjana, la variància, la generalitat o especificitat dels atributs, els valors extrems, etc. La pèrdua d'informació d'unes dades protegides es pot mesurar mitjançant l'observació de les diferències entre les dades originals i les anonimitzades, i mitjançant la premissa que, si hi ha una pèrdua limitada de l'estructura analítica de les dades, això implica que les dades protegides són similars a les dades originals.

**Lectura recomanada**

**Hundepool, A.; Domingo-Ferrer, J.; Franconi, L. *et al.*** (2012). *Statistical disclosure control*. Wiley.

L'anàlisi que s'ha de fer per a avaluar la pèrdua d'informació que ha patit un conjunt de dades protegides variarà segons el conjunt de dades, els mètodes d'anonimització aplicats i com hagin estat aplicats. Atesa la impossibilitat de donar un procediment concret i definitiu per a calcular la pèrdua d'informació, a continuació descriurem les fortaleses i febleses respecte a la preservació de la utilitat de les dades i dels mètodes típics d'anonimització comentats anteriorment:

- Emmascarament no-pertorbatiu: aquests mètodes es caracteritzen per preservar la legitimitat de les dades originals en el conjunt de dades protegides, la qual cosa resulta en un conjunt de registres emmascarats consistents amb els continguts dels registres originals però amb menys detalls. Malgrat mantenir la legitimitat de les dades originals, aquests mètodes incorren generalment en grans pèrdues d'informació perquè es basen a eliminar dades o generalitzar-les destruint-ne el nivell de detall. Per exemple, els va-

lors extrems en un atribut són un dels objectius preferits d'aquests mètodes, que actuen eliminant-los o generalitzant-los de manera que deixin de ser extrems. Tractar els valors extrems és un comportament normal, atès que aquest tipus de valors són «rars» i, per tant, faciliten la reidentificació d'individus; no obstant això, els valors rars també són particularment útils per als investigadors, ja que identifiquen noves àrees de treball, com per exemple malalties «rares». Cal destacar que generalitzar sempre retindrà més quantitat d'informació que eliminar; no obstant això, també cal tenir en compte que la pèrdua d'informació que s'ha patit a l'hora de generalitzar dependrà de la jerarquia de generalització o especialització aplicada: si hi ha poques opcions possibles per a generalitzar un valor a tractar o aquestes generalitzacions són massa generals (podem generalitzar el valor «Audi A3» a «Cotxe», però també podem generalitzar-lo a «Objecte»), la pèrdua d'informació pot ser similar a la d'una eliminació.

- Emmascarament pertorbatiu: els mètodes que pertorben les dades les distorsionen sumant valors aleatoris (afegint soroll), substituint-los per valors agregats prou «representatius» o substituint-los per valors pertanyents a altres registres. En qualsevol cas aquests mètodes acaben generant unes dades protegides que no són legítimes; en altres paraules, són diferents de les originals i poden ser inconsistents respecte a elles en el sentit que es poden donar combinacions il·lògiques de valors d'atributs. Per exemple, suposant que els atributs del conjunt de dades siguin [sexe, malaltia] o [lloc de treball, salari], aquest tipus de mètodes podrien generar unes dades protegides com [dona, càncer de pròstata] o [auxiliar administratiu, 90.000 €] respectivament. Aquests resultats il·lògics poden portar les anàlisis posteriors de les dades protegides a conclusions falses que poden ser més nocives que simplement la pèrdua d'utilitat de les dades generada pels mètodes no-pertorbatius. És per això que en aplicar aquest tipus de mètodes és important controlar el nivell de distorsió introduït en les dades protegides que seran publicades finalment.

Tal com ha dit, la pèrdua de legitimitat de les dades que aquests mètodes apliquen no és un tema menor; no obstant això, un avantatge important d'aquests mètodes és que, depenent de la tècnica concreta aplicada, són bastant efectius a l'hora de preservar certes anàlisis estadístiques. Per exemple, l'*intercanvi de dades* preserva perfectament estadístics com la mitjana, la variància, la distribució de freqüència o els valors extrems; com que la *microagregació* substitueix els valors originals per agregats com la mitjana, la mitjana dels valors protegits quedaria preservada perfectament en aquest cas concret. Finalment, la tècnica d'afegir soroll és capaç de preservar la mitjana de les dades originals i, a més, ofereix una variància proporcional a la variància pròpia del soroll afegit.

- Generació de dades sintètiques: aquests mètodes generen valors nous totalment aleatoris en comparació d'un mètode basat a afegir soroll, en el qual la dada nova té una part original i una part aleatòria (això és, valor original més soroll). Les dades sintètiques tenen el mateix problema que

l'emmascarament pertorbatiu en el sentit que generen dades no legítimes que poden portar a dades protegides il·lògiques i, al seu torn, a conclusions falses i nocives. Respecte a la seva capacitat de preservar estadístics com mitjana, variància, etc., això és determinat directament per com de similars siguin les dades falses generades respecte a les originals. Com que l'estratègia habitual es basa a generar unes dades falses que preservin un determinat estadístic de les dades originals (per exemple, podríem generar uns valors falsos nous per a l'atribut «salari», la mitjana dels quals sigui exactament la mateixa que la mitjana de les dades originals). Una alternativa a aquesta estratègia seria publicar directament la informació estadística que volem preservar. En aquest cas estaríem publicant dades agregades tabulars que no presenten problemes per a la privadesa de les persones i estaríem evitant un procés costós com la generació sintètica d'un conjunt de dades amb escàs valor analític (atès que les dades són falses), més enllà de l'estadístic concret seleccionat.

# 6. Models de privadesa per a microdades

Anteriorment hem indicat que el problema de l'anonimització és produir una taula anonimitzada a partir d'una taula original que satisfaci uns certs requeriments de privadesa determinats pel model de privadesa seleccionat. Els models de privadesa estableixen per endavant unes condicions que les dades protegides han de complir per a garantir un nivell mínim d'anonimitat als *record owners*. En altres paraules, si anonimitzem un conjunt de dades segons un cert model de privadesa, garantirem que les dades protegides resultants oferiran exactament el nivell d'anonimitat promès per aquest model de privadesa. El rol dels mètodes d'anonimització que hem vist en l'apartat anterior és aplicar el model de privadesa que volem sobre les dades que cal protegir.

A continuació explicarem el model de privadesa més cèlebre, la *k*-Anonimitat, un model que ha estat suggerit recentment en una nota pública per l'Agència Espanyola de Protecció de Dades (AEPD) com a eina bàsica per a gestionar el risc de reidentificació. La *k*-Anonimitat és un model de privadesa amb fortaleses rellevants però també amb febleses importants; per això, també parlarem de dues variacions d'aquest model que busquen millorar el seu nivell de protecció: l'*l*-Diversitat i la *t*-Proximitat. Cal destacar que hi ha molts altres models de privadesa en la literatura. No obstant això, no han aconseguit el nivell d'èxit i aplicabilitat de la *k*-Anonimitat per diverses raons; per això, en aquesta documentació ens centrarem en aquest últim model i en les seves variacions més rellevants. El lector interessat pot consultar la literatura d'aquest camp de recerca (per exemple, Benjamin *et al.*, 2010) per conèixer altres models de privadesa.

**Lectura recomanada**

**Benjamin, C. M. F.; Ke Wang, R. C.; Philip, S. Y.** (2010). «Privacy-preserving data publishing: a survey of recent developments». *ACM Computing Surveys* (vol. 42, núm. 4, art. 14).

**Agencia Española de Protección de Datos** (2019). *La k-Anonimidad como medida de la privacidad* [en línia]. <https://www.aepd.es/media/notas-tecnicas/nota-tecnica-kanonimidad.pdf>

## 6.1. *k*-Anonimitat

Aquest model de privadesa (Samarati; Latanya, 1998) assumeix que el conjunt d'atributs que un atacant pot usar per a reidentificar un individu són coneguts (l'atacant els pot obtenir d'alguna font d'informació externa); a partir d'aquí la idea bàsica és ocultar cada registre de dades del conjunt de dades original en un grup de *k*-registres indistingibles entre ells.

**Lectura recomanada**

**Samarati, P.; Latanya, S.** (1998). «Protecting privacy when disclosing information: *k*-anonymity and its enforcement through generalization and suppression». *Informe tècnic*. SRI International.

Entrant una mica més en detalls tècnics, hem explicat anteriorment que les combinacions d'atributs quasiidentificadors són el factor principal de risc de revelació de la identitat; d'aquesta manera, per a evitar la reidentificació de registres en les dades protegides a partir dels quasiidentificadors, **la *k*-Anonimitat requereix com a condició que cada combinació possible de valors dels quasiidentificadors sigui compartida per *k* o més registres**. D'aquesta manera, **anonimitzar sota *k*-Anonimitat garanteix als *record owners* que la probabilitat de reidentificar-los en les dades protegides serà d'1/*k***.

La condició que acabem d'indicar és la que el *data publisher* ha de fer complir en les dades protegides aplicant els mètodes d'emmascarament (pertorbatius o no-pertorbatius) que consideri oportuns per a poder generar un conjunt de dades protegides amb les garanties de la *k*-Anonimitat.

A continuació il·lustrarem la generació d'un conjunt de dades protegides sota aquest model de privadesa utilitzant els mètodes d'anonimització pertorbatius generalització i eliminació, els quals han estat explicats anteriorment i són l'elecció habitual a l'hora d'aplicar aquest model de privadesa (i molts altres). Primer tenim la taula amb les dades originals que volem protegir. Aquestes dades corresponen a una taula de pacients amb les seves malalties diagnosticades. En particular, tenim l'atribut identificador DNI, els atributs quasiidentificadors Edat i Codi postal, i l'atribut confidencial Diagnòstic.

Taula 15. Taula original

| DNI | Edat | Codi postal | Diagnòstic |
|---|---|---|---|
| 37713522Z | 21 | 23058 | Càncer pulmó |
| 36689764P | 24 | 23059 | Càncer pàncrees |
| 67457676C | 26 | 23060 | Càncer còlon |
| 56564576X | 27 | 23061 | Càncer còlon |
| 15434434V | 43 | 23058 | Grip H1N1 |
| 76533777B | 43 | 23059 | Càncer còlon |
| 45646767V | 47 | 23060 | Grip H1N1 |
| 89476473L | 49 | 23061 | Grip H1N1 |
| 64577365S | 32 | 23058 | Càncer còlon |
| 34567646I | 34 | 23059 | Grip H1N1 |
| 78456337R | 35 | 23060 | VIH |
| 58776867D | 38 | 23061 | Càncer pulmó |

A continuació, mostrem la taula protegida mitjançant 4-anonimitat, això és, *k*-Anonimitat quan $k = 4$. D'aquesta manera, ocultarem els registres originals en conjunts indistingibles de 4 registres com a mínim.

Taula 16. Taula protegida sota 4-anonimitat

| DNI | Edat | Codi postal | Diagnòstic |
|---|---|---|---|
| * | 20-30 | 230** | Càncer pulmó |
| * | 20-30 | 230** | Càncer pàncrees |
| * | 20-30 | 230** | Càncer còlon |
| * | 20-30 | 230** | Càncer pulmó |

| DNI | Edat | Codi postal | Diagnòstic |
|---|---|---|---|
| * | 40-50 | 230** | Grip H1N1 |
| * | 40-50 | 230** | Càncer còlon |
| * | 40-50 | 230** | Grip H1N1 |
| * | 40-50 | 230** | Grip H1N1 |
| * | 30-40 | 230** | Càncer còlon |
| * | 30-40 | 230** | Grip H1N1 |
| * | 30-40 | 230** | VIH |
| * | 30-40 | 230** | Càncer pulmó |

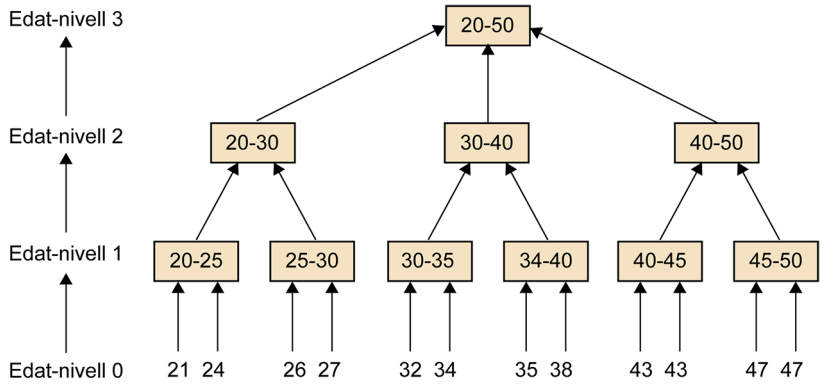
La taula protegida és solament una de les possibles versions que obtindríem aplicant 4-anonimitat mitjançant generalització i eliminació. Diferents maneres d'aplicar aquestes dues tècniques generaran diferents versions d'aquesta taula. Cal destacar que en la literatura també s'utilitza el mètode no-pertorbatiu microagregació per a generar taules protegides sota *k*-Anonimitat (Domingo-Ferrer, 2016); aplicant aquest mètode d'anonimització, també es generarien diferents versions d'aquesta taula. En tot cas, el que hem fet en aquesta taula és, primer, eliminar l'atribut identificador (DNI), atès que permetia la reidentificació directa de cada registre, i, a continuació, generalitzar els atributs quasiidentificadors (Edat i Codi postal) reduint la quantitat d'informació que proporcionen fins a aconseguir que cada combinació de valors sigui compartida per quatre registres com a mínim (la condició que ens exigia la 4-anonimitat).

**Lectura recomanada**

**Domingo-Ferrer, J.; Sánchez, D.; Soria-Comas, J.** (2016). *Database anonymization: privacy models, data utility, and microaggregation-based inter-model connections*. Morgan & Claypool Publishers.

Respecte a la generalització aplicada a les dades originals, en la figura 2 es mostra la jerarquia de generalització per a l'atribut Edat. Els valors corresponents al nivell 0 són els valors originals. En la generalització aplicada a aquest atribut hem arribat fins al nivell 2 en la jerarquia, en el qual treballem amb rangs de 10 elements.

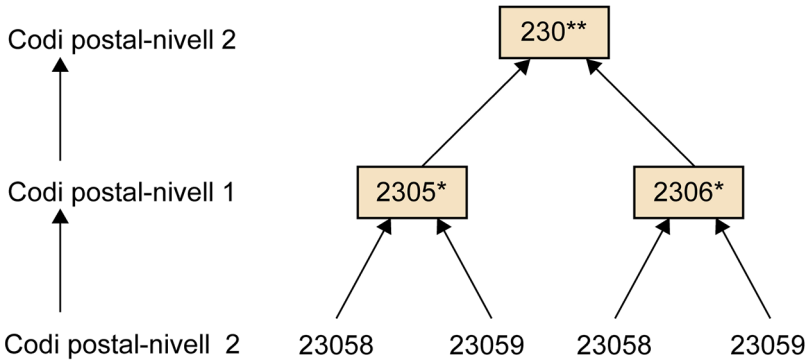
Figura 2. Jerarquia de generalització per a l'atribut Edat




Font: elaboració pròpia (adaptat de Domingo-Ferrer, 2016)

Per a l'atribut Codi postal, hem utilitzat la jerarquia de generalització que es mostra en la figura 3. En la generalització aplicada a aquest atribut hem arribat fins al nivell 2 en la jerarquia, el qual engloba els quatre codis postals existents en les dades originals.

Figura 3. Jerarquia de generalització per a l'atribut Codi postal




Font: elaboració pròpia (adaptat de Domingo-Ferrer, 2016)

Ara, partint d'aquesta taula protegida, imaginem que tenim un atacant que intenta descobrir la malaltia que han diagnosticat a un cert individu. Imaginem que aquest atacant sap que l'individu en qüestió té un registre vinculat en la taula protegida, que té 34 anys i que viu al barri amb codi postal 23059. Amb la combinació de dades que l'atacant té, en la taula apareixen quatre registres diferents que podrien correspondre a l'individu buscat. L'atacant no té manera de saber exactament quin d'aquests quatre registres corresponen al seu objectiu. Com a resultat d'això, l'única informació que aconsegueix l'atacant és que el seu objectiu ha estat diagnosticat amb una de les malalties que apareixen en aquest grup de quatre registres.

Un factor molt important a tenir en compte en aplicar aquest model de privadesa és el valor del paràmetre $k$. Aquí entren en joc dos factors: la utilitat de les dades protegides i el nivell de privadesa que volem donar als *record owners*. Pel que fa a la utilitat, en la taula protegida podem veure que el fet d'haver utilitzat un $k = 4$ ens ha obligat a utilitzar un cert nivell de generalització (pèrdua d'informació) precisament per a poder construir grups de quatre registres indistingibles. Aconseguir una protecció $k = 2$ hauria estat més senzill i requerit menys generalització, amb la qual cosa la taula protegida retindria més informació, seria més útil. De la mateixa manera, aconseguir una protecció $k = 6$ hauria requerit generalitzar encara més els quasiidentificadors i generat una taula protegida amb menys informació i menys útil. Pel que fa a la privadesa, tenim la probabilitat de reidentificació d'$1/k$ que garanteix aplicar $k$-Anonimitat. En aquest cas, un $k = 2$ donaria a l'atacant el 50% de probabilitats de reidentificar l'individu en les dades protegides. Per contra, un $k = 6$ donaria a l'atacant el 16% de probabilitats de tenir èxit en el seu atac. Com podem veure, com més valors de $k$ major garantia d'anonimitat i major pèrdua d'utilitat en les dades protegides, i viceversa. Com a conclusió, el paràmetre $k$

s'hauria de seleccionar buscant l'equilibri entre tots dos factors. No hi ha una resposta concreta sobre quin valor de *k* és el millor; dependrà simplement de les circumstàncies.

El principal avantatge del model *k*-Anonimitat i la raó per la qual s'explica el seu èxit respecte a altres models existents en la literatura són que proporciona una noció molt intuïtiva de la limitació del risc de revelació: si ocultem un cert registre dins un conjunt de *k* registres indistingibles, tenim una probabilitat de l'1/*k* de reidentificar aquest registre. És un concepte intuïtiu i fàcil d'entendre. No obstant això, aquesta protecció resulta insuficient quan els registres dins el grup *k*-anònim tenen un valor similar per a l'atribut confidencial. Per exemple, seguint amb la taula protegida sota 4-anonimitat anterior, tenim un primer conjunt de quatre registres en què les malalties diagnosticades són càncers de diferents òrgans. Si l'atacant sap que un d'aquests registres correspon a un cert individu, pot inferir sense error que té càncer. En aquest cas senzill podem veure que el *k*-anonimat brinda protecció contra la revelació d'identitat: l'atacant no pot saber quin registre està vinculat amb l'individu; solament ho pot «encertar» amb una probabilitat d'1/4. No obstant això, aquesta protecció és insuficient per a evitar el risc de revelació de l'atribut quan els valors de l'atribut confidencial són similars en tots els registres: l'atacant no necessita reidentificar el registre per a saber que l'individu té càncer.

En aquest sentit, en la literatura s'han proposat dos atacs per al model de privadesa *k*-Anonimitat que exploten la falta de variabilitat en l'atribut confidencial:

- Atac d'homogeneïtat (en anglès, *homogeneity attack*): tal com s'ha comentat, si tots els registres en un grup *k*-anònim comparteixen el mateix valor per a l'atribut confidencial, la *k*-Anonimitat no proporciona cap protecció contra la revelació d'atributs.

- Atac amb coneixement d'antecedents (en anglès, *background knowledge attack*): aquest atac pot tenir lloc en grups de *k* registres on hi ha poca variabilitat en els valors de l'atribut confidencial i l'atacant té algun tipus de coneixement addicional sobre l'individu objecte de l'atac. Per exemple, en el segon grup de la taula protegida sota 4-anonimitat tenim tres registres amb «Grip H1N1» i un registre amb «Càncer còlon»; la baixa variabilitat ja fa que l'atacant sense informació addicional tingui el 50% de probabilitats d'encertar la malaltia que té l'usuari (en lloc del 25% que ofereix teòricament la 4-anonimitat), però, a més, si l'atacant té alguna informació extra que li permet, per exemple, descartar el càncer, sabrà amb el 100% de certesa que l'individu té «Grip H1N1»

### 6.2. *l*-Diversitat

**Lectura recomanada**

**Machanavajjhala, A.; Kifer, D.; Gehrke, J. *et al.*** (2007). «*l*-diversity: privacy beyond *k*-anonymity». *ACM Transactions on Knowledge Discovery from Data* (vol. 1, núm. 1).

En un intent per a mitigar els problemes que la *k*-Anonimitat té a l'hora d'oferir protecció contra la revelació de l'atribut, els autors de «*l*-diversity: privacy beyond *k*-anonymity» proposen el model de privadesa conegut com a *l*-Diversitat.

L'objectiu d'aquest model és exigir un nivell mínim de diversitat per als valors d'atribut confidencial en cadascun dels grups de registres *k*-anònims. Aquest nivell mínim de diversitat requerit el marca el paràmetre *l*. En particular, **la condició necessària perquè un grup de registres compleixi l'*l*-Diversitat és que hi hagi almenys *l* valors diferents ben representats en l'atribut confidencial**. Aquesta condició l'han de complir tots els grups de registres indistingibles de la taula protegida.

La indicació que ha d'haver-hi *l* valors diferents «ben representats» és bastant vaga i ha portat en la pràctica a diverses definicions complementàries. Per exemple, la definició de *l*-Diversitat més senzilla seria la coneguda com a *distinct l-diversity*, la qual demana simplement que en el grup de registres anonimitzat apareguin *l* valors diferents per a l'atribut confidencial. Una altra definició més complexa seria la d'*entropy l-diversity*, en la qual es calcula l'entropia (això es podria explicar com la «incertesa» o el «caos» que un element o conjunt d'elements proporciona; com més «caos» més variabilitat) conjunta que proporcionen els valors de l'atribut confidencial. Aquesta entropia conjunta ha de ser igual o superior al llindar que marca el paràmetre *l*.

Centrant-nos en la definició de *Distinct l-Diversity* i en la taula d'exemple protegida sota *4*-anonimitat, podem veure que el segon grup compliria solament 2-diversitat, atès que solament hi ha dos valors possibles en l'atribut confidencial: «Grip H1N1» i «Càncer de còlon». Respecte als altres grups de registres, el primer conjunt compliria 3-diversitat i el tercer conjunt compliria 4-diversitat. En total, la taula anonimitzada en la seva composició actual garantiria solament 2-diversitat (el valor més baix de tots els grups).

Si volguéssim generar una versió d'aquesta taula protegida sota 4-Diversitat, hauríem d'aplicar més generalització a l'atribut Edat (amb la pèrdua d'informació que això comporta). D'aquesta manera, podríem tenir la taula anonimitzada següent deixant solament dues opcions per a l'Edat (major de 35 anys i menor de 35 anys) i obtenint dos grups de registres en lloc de tres.

Taula 17. Taula protegida sota 4-diversitat

| DNI | Edat | Codi postal | Diagnòstic |
|---|---|---|---|
| * | <35 | 230** | Càncer pulmó |
| * | <35 | 230** | Càncer pàncrees |
| * | <35 | 230** | Càncer pulmó |

| DNI | Edat | Codi postal | Diagnòstic |
|---|---|---|---|
| * | <35 | 230** | Càncer còlon |
| * | <35 | 230** | Càncer còlon |
| * | <35 | 230** | Grip H1N1 |
| * | >35 | 230** | Grip H1N1 |
| * | >35 | 230** | Càncer còlon |
| * | >35 | 230** | Grip H1N1 |
| * | >35 | 230** | Grip H1N1 |
| * | >35 | 230** | VIH |
| * | >35 | 230** | Càncer pulmó |

Tal com hem vist, l'*l*-Diversitat intenta mitigar el risc de revelació de l'atribut en requerir un mínim nivell de variabilitat en els valors de l'atribut confidencial per a cada grup de registres. No obstant això, aquest model no és completament satisfactori, ja que és vulnerable a dos atacs ben documentats en la literatura (Domingo-Ferrer, 2016):

**Lectura recomanada**

**Domingo-Ferrer, J.; Sánchez, D.; Soria-Comas, J.** (2016). *Database anonymization: privacy models, data utility, and microaggregation-based inter-model connections*. Morgan & Claypool Publishers.

- Atac d'asimetria (en anglès, *skewness attack*): per donar la menor quantitat d'informació possible sobre l'atribut confidencial vinculat a un individu en concret, *l*-Diversitat força que en cada grup de registres aparegui un nombre mínim de valors diferents. En aquest sentit la situació ideal per a aquest model de privadesa seria que en cada grup de registres cada valor possible tingués la mateixa freqüència d'aparició; això és, si tenim quatre valors possibles per a un atribut, l'ideal seria que aquests quatre valors fossin representats amb la mateixa proporció en tots els grups de registres de la taula protegida (és a dir, al 25% cada valor). D'aquesta manera, un atacant no guanyaria cap informació sobre l'atribut confidencial protegit d'un individu en concret: qualsevol dels quatre valors podria correspondre a aquesta persona.

  Aquesta situació ideal, encara que en aparença sigui perfecta per a la privadesa dels *record owners*, pot ser contraproduent per a ells si la proporció utilitzada en els grups protegits per als valors de la variable confidencial és molt asimètrica respecte a la proporció d'aparició d'aquests valors en el conjunt de dades original (o al món en general). Per a visualitzar aquest problema, imaginem una taula de pacients d'un hospital on l'atribut confidencial registra la presència o absència d'una malaltia determinada. Suposem que en la taula de dades original la incidència de la malaltia en qüestió és de l'1%; així, doncs, el 99% d'individus vinculats a aquesta taula estan lliures d'aquesta malaltia. Si protegim aquesta taula sota *2*-diversitat, el que intentarem és que en cada grup de registres protegits la proporció d'aparició de la malaltia sigui del 50%. D'aquesta manera, si un atacant és capaç de vincular un cert individu amb un dels grups de registres protegits inferirà, encara que no es pugui reidentificar el registre concret, que

l'individu té el 50% de probabilitats de patir la malaltia, la qual cosa és un problema seriós tenint en compte que les probabilitats reals de patir aquesta malaltia en la taula original són de l'1%. En altres paraules, el sol fet d'aparèixer en la taula protegida amb *l*-Diversitat s'ha convertit en un problema per als *record owners,* atès que el model de privadesa ha «forçat» una sobrerepresentació d'un valor en concret de l'atribut confidencial en les dades protegides.

- Atac de similitud (en anglès, *similarity attack*): tal com s'ha dit, *l*-Diversitat busca com a ideal que els valors possibles de l'atribut confidencial quedin representats amb la mateixa proporció en tots els grups de registres de la taula protegida. Un problema significatiu de l'aplicació pràctica d'aquest model és que a l'hora d'avaluar la diversitat de valors en un grup de registres anonimitzat no es té en compte la distància semàntica entre els valors: es considera simplement que si els valors són diferents hi ha diversitat. Ens podem adonar del problema que això comporta en veure la taula protegida sota *4*-diversitat: en el primer grup tenim quatre malalties teòricament diferents (tenen noms diferents), però tres d'aquestes malalties són «càncer»; de fet, dels sis registres, cinc estan vinculats amb la malaltia «càncer» (són valors similars a la pràctica). Si sabem que un individu està ocult en aquest grup de registres, podem inferir que té càncer amb el 83% de probabilitat, la qual cosa ens indica que la *l*-Diversitat no té èxit a l'hora de protegir la seva privadesa.

### 6.3. *t*-Proximitat

**Lectura recomanada**

Sobre el model de privadesa:
**Li, N.; Li, T.; Venkatasubramanian, S.** (2007). «*t*-closeness: privacy beyond *k*-anonymity and *l*-diversity». *ICDE* (pàg. 106-115). IEEE.

Aquest model de privadesa és un refinament de l'*l*-Diversitat. En el cas de l'*l*-Diversitat s'intentava representar tots els valors de l'atribut confidencial amb igual proporció en cada grup de registres protegits, la qual cosa comporta els problemes que ja hem comentat. **En el cas de la *t*-Proximitat, la condició que cal complir és que en cada grup de registres protegits els possibles valors de l'atribut confidencial apareguin en la mateixa proporció en què apareixien en la taula original (o al més semblant possible segons el paràmetre *t*).**

Tornant a l'exemple introduït en explicar l'atac d'asimetria de l'*l*-Diversitat, en aquest cas la *t*-Proximitat buscarà que en cada grup de registres es mantingui la proporció d'aparició de la malaltia d'1% positius i 99% negatius. Igualment, la *t*-Proximitat no té problemes relacionats amb la distància semàntica entre valors. Per a visualitzar això, imaginem que el grup anonimitzat en què cinc dels sis registres apuntaven a «càncer» estigués protegit sota *t*-Proximitat (en lloc d' *l*-Diversitat). *t*-Proximitat «força» que les proporcions es mantinguin en els grups protegits respecte a la taula original; per tant, si *t*-Proximitat ha generat un grup protegit en què el 83% de registres apunten a diferents tipus de «càncer», tenim la certesa que en la taula original el 83% dels registres també apunten a diferents tipus d'aquesta malaltia i, a més, tenim la certesa

que les proporcions de diferents tipus de càncer també es mantenen; per tant, un atacant no pot aprendre res de nou simplement per saber que un individu està vinculat a un cert grup de registres protegits.

El paràmetre *t* d'aquest model és un llindar que defineix la distància màxima entre la distribució de valors en la taula original i la distribució de valors en els grups protegits que estem disposats a tolerar. Entenem aquesta distància entre distribucions com la quantitat de similaritat que tenen. En la definició d'aquest model de privadesa no s'indica una mètrica de distàncies de distribucions en concret, encara que generalment s'utilitza la mètrica *Earth Mover's Distance (EMD)* (Rubner; Tomasi; Guibas, 2000). Cal dir que la situació ideal seria buscar una protecció de les dades sota $t = 0$, la qual cosa implicaria que les dades protegides han aconseguit preservar exactament les proporcions existents en les dades originals; no obstant això, arribar a aquest nivell d'anonimització ideal implicarà generalment aplicar una forta generalització i eliminació a les dades, amb la consegüent pèrdua d'utilitat.

**Lectura recomanada**

**Rubner, Y.; Tomasi, C.; Guibas, L. J.** (2000). «The earth mover's distance as a metric for image retrieval». *International Journal of Computer Vision* (vol 40, núm. 2, pàg. 99-121).

# 7. Anonimització d'altres tipus de dades

En els apartats anteriors hem tractat l'anonimització de microdades emmagatzemades en bases de dades estadístiques. En aquest tipus de bases de dades la informació és estructurada perfectament i sempre podem trobar un conjunt d'atributs quasiidentificadors i atributs confidencials fix, relativament petit i amb uns valors concrets i ben definits. Per exemple, en les taules d'exemple que hem utilitzat fins ara es podien veure dos o tres atributs quasiidentificadors que corresponien a elements molt concrets, com Edat, Sexe o Codi postal, els quals tenen uns valors possibles específics i clars. En aquestes taules també podíem veure un atribut confidencial diferenciat molt clarament de la resta, atès que reflectia una informació objectivament confidencial, com un diagnòstic mèdic o el salari. Depenent de la taula en qüestió, el nombre d'atributs d'un tipus o un altre pot variar, però en qualsevol cas sabem que una taula en concret sempre tindrà un nombre d'atributs determinat per a cadascun dels seus registres; i també podrem distingir un atribut quasiidentificador d'un atribut confidencial.

Ens hem centrat en aquest tipus d'estructura de dades, atès que és la més típica a l'hora de gestionar la informació i publicar-la per al seu ús per part de tercers (Domingo-Ferrer, 2016); no obstant això, cal destacar que, tot i que sigui la manera més típica de manejar dades, hi ha altres opcions que mereixen certa atenció. Aquestes altres opcions, encara que treballin igualment sobre taules (les taules són una forma habitual de gestió de dades en la informàtica), tenen diferències importants respecte al que hem vist fins ara. En particular, veurem que en certs tipus de dades pot haver-hi registres que tinguin més atributs que uns altres, o pot passar que no sapiguem diferenciar un atribut confidencial d'un quasiidentificador.

**Lectura recomanada**

**Domingo-Ferrer, J.; Sánchez, D.; Soria-Comas, J.** (2016). *Database Anonymization: Privacy Models, Data Utility, and Microaggregation-based Inter-model Connections*. Morgan & Claypool Publishers.

També és important destacar que, tot i tractar-se d'altres maneres d'estructurar la informació, els mètodes d'anonimització de microdades més habituals que hem vist, com la generalització o l'eliminació, continuen tenint aplicació a aquests altres tipus de dades; i els models de privadesa vistos anteriorment, com la *k*-Anonimitat, també poden ser utilitzats aplicant algun tipus de modificació. Per tant, el lector ha de veure aquest apartat com una extensió del que ja ha vist, en el qual es tracten particularitats que es poden trobar en el camp de la publicació de dades.

En concret, a continuació revisarem la problemàtica associada a l'anonimització de dades transaccionals, de moviment d'objectes i de dades textuals, les quals, encara que siguin menys freqüents que les microdades utilitzades en bases de dades estadístiques, són prou comunes i delicades des del punt de vista de la privadesa per a ser considerades.

**Lectura recomanada**

**Benjamin, C. M. F.; Ke Wang, R. C.; Philip, S. Y.** (2010). «Privacy-preserving data publishing: a survey of recent developments». *ACM Computing Surveys* (vol. 42, núm. 4, art. 14).

### 7.1. Dades transaccionals

Les dades transaccionals es caracteritzen per tenir un conjunt d'atributs de nombre variable i per la dificultat de distingir atributs quasiidentificadors dels confidencials fins al punt de considerar-los quasiidentificadors i confidencials simultàniament. L'exemple típic de dades transaccionals és el de registres de compradors que han adquirit una sèrie d'ítems (en una botiga en línia com Amazon o amb una compra feta en una botiga física com un supermercat).

Un exemple gràfic sobre aquest tipus de dades i els problemes de privadesa que plantegen es pot trobar a «Privacy-preserving anonymization of set-valued data». D'aquesta manera, considerem una base de dades d'un supermercat que emmagatzema les compres fetes pels diferents compradors. Considerem també la persona Bob que ha comprat cafè, pa, formatge gouda, llet, te i una bombeta al supermercat. Al supermercat aquesta compra ha generat un registre transaccional amb un cert identificador («12345» en la taula d'exemple) de la compra, i el conjunt d'ítems comprats. Aquest registre s'emmagatzema en la base de dades juntament amb els registres transaccionals generats per altres clients:

**Lectura recomanada**

**Terrovitis M.; Mamoulis N.; Kalnis, P.** (2008). «Privacy-preserving anonymization of set-valued data». *Proceedings of the VLDB Endowment* (vol. 1, pàg. 115-125).

Taula 18

| ID | Compra |
|---|---|
| 12345 | {cafè, pa, formatge gouda, llet, te, bombeta} |
| 34543 | {llet, lleixiu} |
| 55435 | {galetes, suc de taronja, pa} |

En la taula de dades original el primer que podem veure és que l'atribut Compra és molt diferent dels atributs que ens trobàvem en les taules de microdades. El valor que pot tenir aquest atribut és totalment variable tant en el nombre d'ítems com en la combinació d'ítems seleccionat: podem tenir valors per a l'atribut Compra que siguin únics, és a dir, pot ocórrer passar que una persona compri una combinació d'ítems que no hagi comprat ningú més. Això representa un fort contrast respecte als atributs com Sexe o Diagnòstic que hem vist en les microdades; en aquests atributs el valor corresponia a un conjunt d'opcions bastant limitat (concretament, Sexe solament admetia dues opcions), i el valor era únic obligatòriament. Amb les dades transaccionals, en canvi, podem tenir un atribut amb un valor, o diversos, i aquests poden

correspondre a un conjunt d'opcions enorme, i que és relativament fàcil que augmenti amb el temps o que canviï (un supermercat porta nous productes i n'elimina d'altres periòdicament).

Seguint amb l'exemple, imaginem que Bob va amb la seva compra a l'autobús i un atacant pot veure una part de la seva compra: cafè, pa i bombeta. Posteriorment, el supermercat publica la base de dades transaccionals eliminant els atributs identificadors (aquest continuaria essent el primer pas en qualsevol procés d'anonimització, siguin microdades o qualsevol altre tipus de dades):

Taula 19

| ID | Compra |
|---|---|
| * | {**cafè**, **pa**, formatge gouda, llet, te, **bombeta**} |
| * | {llet, lleixiu} |
| * | {galetes, suc de taronja, **pa**} |

L'atacant pot comprovar la llista d'ítems que sap que Bob va comprar amb tots els registres de la taula publicada, i si aquesta combinació solament apareix en un únic registre tindrà la certesa al 100% que aquest registre correspon a Bob (revelació d'identitat) i podrà conèixer la llista completa d'ítems que ha comprat (revelació d'atribut). En aquest cas és important veure com l'atribut Compra actua simultàniament d'atribut confidencial (els elements comprats són l'element confidencial de les dades) i d'atribut quasiidentificador, ja que és la combinació de valors d'aquest atribut el que porta a la reidentificació del registre.

Cal destacar que aquest tipus de dades i la seva problemàtica associada apareixen sempre que tenim atributs que poden prendre com a valors un conjunt d'elements variable i múltiple; no estan limitats a la compra d'ítems en botigues. Per exemple, els *query logs* d'AOL que hem vist al principi d'aquest document són un altre exemple típic de dades transaccionals. En concret, una consulta com «*dog cornea treatment*», enviada al motor de cerca AOL, es registraria així:

Taula 20

| Pseudònim | Consulta |
|---|---|
| 2178 | {*dog, cornea, treatment*} |

Veiem que tenim l'atribut Consulta, el qual pren com a valor un conjunt d'elements variable i múltiple, en aquest cas format pels substantius que formaven la consulta. Es pot veure la semblança d'aquest tipus de dades amb l'exemple de la compra al supermercat.

Una manera habitual de protegir aquest tipus de dades es descriu a «Privacy-preserving anonymization of set-valued data» i passa per aplicar generalització i eliminació, tal com es feia en els conjunts de microdades. En l'exemple que hem vist, la generalització que podríem fer és substituir «cafè», «llet» i «suc de taronja» per un ítem més general anomenat «beguda esmorzar». Respecte a l'eliminació, podríem eliminar «bombeta» assumint per a l'exemple que és un element molt «rar» en la base de dades original (molt poca gent el compra). La taula resultant quedaria així:

**Lectura recomanada**

**Terrovitis M.; Mamoulis N.; Kalnis, P.** (2008). «Privacy-preserving anonymization of set-valued data». *Proceedings of the VLDB Endowment* (vol. 1, pàg. 115-125).

Taula 21

| ID | Compra |
|---|---|
| * | {**beguda esmorzar**, **pa**, formatge gouda, llet, te} |
| * | {**beguda esmorzar**, lleixiu} |
| * | {galetes, **beguda esmorzar**, **pa**} |

Si l'atacant accedeix a aquesta taula, amb la informació parcial que té (cafè, pa i bombeta) i sabent que cafè equival a «beguda esmorzar», veurà dos registres diferents que podrien correspondre a Bob, amb la qual cosa ja es reduiria el risc de revelació. Aplicant més generalització i eliminació, es podria reduir encara més aquest risc a costa de reduir la utilitat de les dades protegides (a semblança del que hem vist amb les microdades).

Cal destacar que un model de privadesa que en la literatura es planteja per protegir dades transaccionals és la $k^m$-Anonimitat, una variació de la *k*-Anonimitat, en la qual, assumint que l'atacant coneix un màxim d'*m* ítems d'una transacció específica, s'evitarà que pugui reidentificar aquesta transacció en un grup de *k* transaccions protegides.

**Lectura recomanada**

Sobre $k^m$-Anonimitat:

**Terrovitis M.; Mamoulis N.; Kalnis, P.** (2008). «Privacy-preserving anonymization of set-valued data». *Proceedings of the VLDB Endowment* (vol. 1, pàg. 115-125).

### 7.2. Dades de moviment d'objectes

Les dades de moviment d'objectes i persones estan relacionades directament amb els serveis basats en localització (en anglès, *location-based services*, LBS), serveis que treballen amb les posicions físiques que ocupen en certs instants de temps els objectes o individus i amb certa informació de context o personal. Cal dir que una seqüència de múltiples posicions físiques visitades en certs instants de temps correspon a una trajectòria. En vista d'aquestes característiques, podem concloure que les dades de moviment dels objectes o persones tenen les particularitats següents: depenen de la localització, depenen del temps i es generen en grans quantitats.

Un exemple gràfic sobre aquest tipus de dades i els problemes de privadesa que plantegen és el següent (Benjamin *et al.*, 2010). Un hospital vol publicar una taula de dades de pacients que conté: 1) un identificador del pacient; 2) les seves trajectòries a la ciutat on resideixen, i 3) la malaltia que se'ls ha diagnosticat. La taula amb les dades originals quedaria de la manera següent:

**Lectura recomanada**

**Benjamin, C. M. F.; Ke Wang, R. C.; Philip, S. Y.** (2010). «Privacy-preserving data publishing: a survey of recent developments». *ACM Computing Surveys* (vol. 42, núm. 4, art. 14).

Taula 22

| DNI | Trajectòria | Diagnòstic |
|---|---|---|
| 37713522Z | A1 → D2 → B3 → E4 → F6 → C7 | VIH |
| 36689764P | B3 → E4 → F6 → E8 | Grip H1N1 |
| 67457676C | B3 → C7 → E8 | Grip H1N1 |
| 56564576X | D2 → F6 → C7 → E8 | Al·lèrgia |
| 15434434V | D2 → C5 → F6 → C7 | VIH |
| 76533777B | C5 → F6 → E9 | Càncer còlon |

La trajectòria d'un individu és una seqüència de múltiples parelles de localització i instant de temps. La localització queda representada com una lletra que, per exemple, pot equivaler a una posició específica GPS o un carrer o un barri, etc. L'instant de temps queda representat com un número que codifica una *data* + *hora* determinada, que, per exemple, pot equivaler a 14/08/2019 + 20:07. Com que la quantitat de localitzacions és variable i diferent per a cada registre, tenim una situació similar a la del cas de les dades transaccionals. Però en aquest cas l'atribut confidencial (el diagnòstic) i l'atribut quasiidentificador (la trajectòria) són diferenciats *a priori*.

Seguint amb l'exemple, imaginem que un atacant té accés a una versió de la taula anterior en la qual l'única mesura de protecció aplicada ha estat eliminar el DNI dels pacients. Imaginem també que l'atacant sap que el seu objectiu, Alice, ha visitat E a l'instant 4, i C a l'instant 7.

Taula 23

| DNI | Trajectòria | Diagnòstic |
|---|---|---|
| * | A1 → D2 → B3 → **E4** → F6 → **C7** | VIH |
| * | B3 → **E4** → F6 → E8 | Grip H1N1 |
| * | B3 → C7 → E8 | Grip H1N1 |
| * | D2 → F6 → **C7** → E8 | Al·lèrgia |
| * | D2 → C5 → F6 → **C7** | VIH |
| * | C5 → F6 → E9 | Càncer còlon |

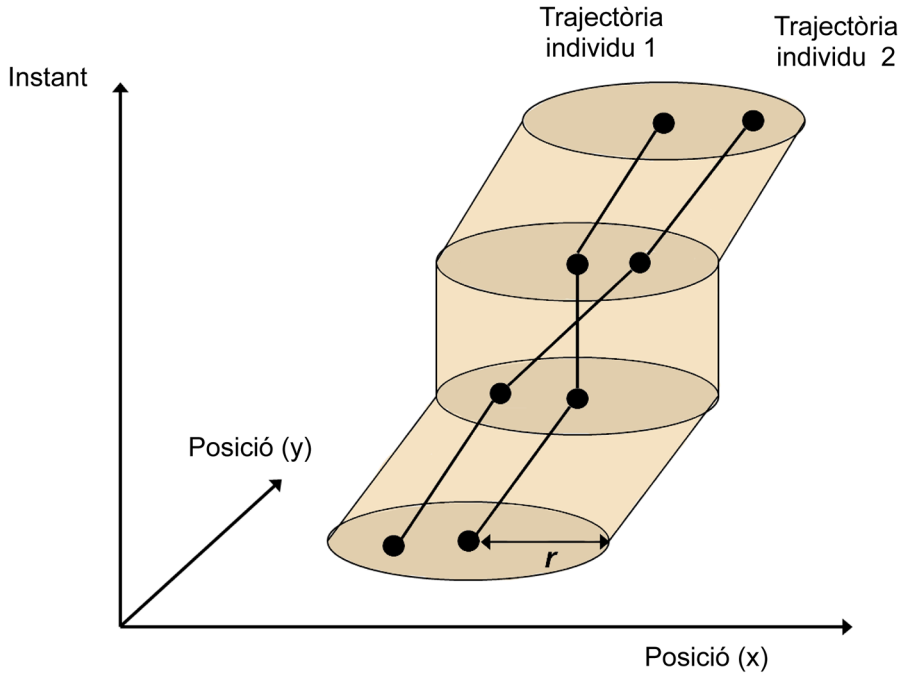
Amb aquesta informació parcial, l'atacant és capaç de reidentificar el registre pertanyent a Alice, atès que solament una trajectòria de la taula conté aquestes dues localitzacions als instants indicats. Com a resultat, tenim una revelació d'identitat que porta, a més, a revelar també el diagnòstic d'Alice.

Imaginem ara que l'objectiu de l'atacant és Bob en lloc d'Alice i que sap que Bob ha estat en la localització D a l'instant 2, i en la localització F a l'instant 6. En aquest cas l'atacant troba tres registres que poden correspondre a Bob (el primer, el quart i el cinquè). En aquesta situació l'atacant no pot reidentificar el registre vinculat a Bob, però pot inferir que Bob té VIH amb el 67% de probabilitat. En aquest cas tenim un risc clar de revelació de l'atribut, que pot acabar en el 100% d'èxit en cas que l'atacant tingui algun coneixement addicional sobre el tipus de malaltia que té Bob.

Com a resultat, podem veure que les dades de moviment d'objectes són lleugerament diferents de les dades que hem vist fins ara, però també podem veure que tenen semblances importants amb dades transaccionals i amb microdades. De fet, comparteixen els mateixos problemes respecte als riscos de revelació i l'efecte del coneixement d'antecedents que pugui tenir l'atacant. De la mateixa manera que s'ha intentat anonimitzar microdades i dades transaccionals, en el cas de les dades de moviment el procés d'anonimització més habitual també passa per aplicar generalització i eliminació als punts de les trajectòries amb una adaptació de la *k*-Anonimitat. En particular, en aquest cas la idea bàsica és crear una àrea d'incertesa segons un cert radi *r* al voltant de les posicions físiques mitjançant *generalització* (per exemple, si la localització real és un carrer, podríem generalitzar-la a un barri) i, d'aquesta manera, aconseguir que dins d'aquesta àrea d'incertesa coincideixin *k* individus diferents en un cert instant de temps.

La figura 4 representa visualment dues trajectòries originals corresponents al moviment de dos individus diferents protegides mitjançant *2*-anonimitat per a dades de moviment d'objectes. La generalització de les dades originals (per exemple, generalitzar les coordenades GPS exactes al barri de la ciutat que engloba aquestes posicions GPS) queda representada com una àrea d'incertesa al voltant dels punts de localització, de manera que aquesta àrea substitueix les posicions exactes i fa que els dos individus apareguin en les dades protegides ocupant el mateix lloc al mateix instant de temps. D'aquesta manera, s'aconsegueix l'anonimització de les seves trajectòries (assumint la pèrdua d'informació o utilitat corresponent).

Figura 4. Anonimització de dades de moviment d'individus




Font: elaboració pròpia (adaptat de Benjamin *et al.*, 2010).

### 7.3. Dades textuals

Els tipus de dades anteriors no eren totalment estructurats com les microdades, ja que teníem atributs que podien prendre un nombre de valors múltiple i indefinit i, en certes circumstàncies, podia ser complicat distingir els atributs quasiidentificadors dels confidencials. Així i tot, aquestes dades continuaven mantenint prou estructura per a ser representades amb taules, igual que fèiem amb les microdades. De la mateixa manera, l'anonimització d'aquests tipus de dades, que podríem anomenar «semiestructurades», acaba essent bastant similar a la protecció que apliquem a les microdades, això és, usem els mateixos mètodes d'anonimització (generalització i eliminació), i la *k*-Anonimitat (més o menys adaptada) continua essent el model de privadesa habitual.

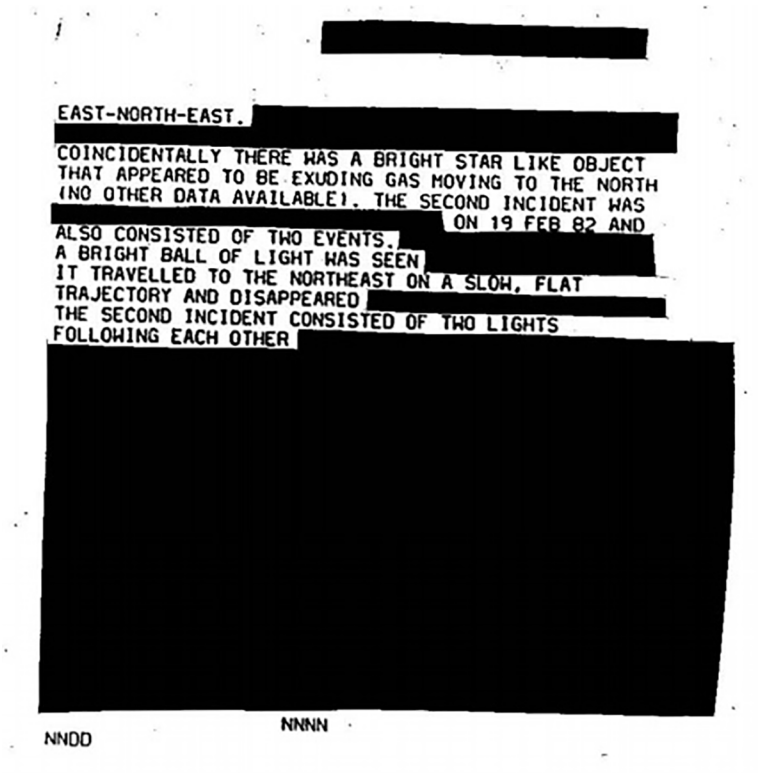
En contrast amb tot el que s'ha vist anteriorment, tenim les dades textuals, enteses com a documents de text en el qual apareixen referències a individus i a dades personals seves que es poden considerar confidencials. Aquestes dades no poden ser representades com a taules, ja que són text lliure, no tenen atributs i tampoc hi ha un conjunt limitat de valors. En la literatura aquests tipus de dades s'anomenen «no-estructurades» i es consideren molt difícils de tractar atesa la complexitat d'avaluar si un cert text (una paraula, una frase o un paràgraf sencer) és una amenaça a la privadesa d'algun individu.

**Lectura recomanada**

**Sánchez, D.; Batet, M.; Viejo, A.** (2013). «Automatic general-purpose sanitization of textual documents». *IEEE Transactions on Information Forensics and Security* (vol. 8, núm. 6, pàg. 853-862).

L'anonimització de dades textuals s'ha basat tradicionalment a redactar els elements del text que es podien considerar perillosos. Redactar és eliminar els elements triats del text substituint-los per una marca negra. Podem veure un exemple del resultat de redactar un document en la figura 5.

Figura 5. Document redactat




Tradicionalment, el procés de redacció és un mètode manual, això és, un expert ha de llegir el text i destriar quins elements són perillosos i quins són innocus. A part del propi coneixement de l'expert, també hi ha guies sobre els elements que han de ser eliminats. Per exemple, en el context mèdic tenim les regles *HIPAA (Health Insurance Portability and Accountability Act)* proposades pels Estats Units el 1996, que indiquen exactament quins elements identifiquen directament una persona (nom, número de seguretat social, etc.) i, per tant, han de ser eliminats de qualsevol text prèviament a la seva publicació. Cal destacar que, tot i les diferències entre dades textuals i microdades, podem veure que al final el comportament a l'hora d'anonimitzar és similar: en les microdades eliminàvem els atributs identificadors de les taules, en les dades textuals eliminem qualsevol paraula o frase que pugui identificar una persona.

**Lectura recomanada**

**Department of Health and Human Services, Office of the Secretary** (2000). *The Health Insurance Portability and Accountability Act of 1996*. Tech. Rep. Federal Register 65 FR 82462.

El problema de l'anonimització manual de documents utilitzada tradicionalment és doble: 1) anonimitzar manualment tots els documents que es publiquen en entorns oberts com internet ja és inabastable a dia d'avui, i fer-ho en el futur, quan absolutament tot es publicarà en format digital i es generaran fàcilment informes textuals de gairebé qualsevol cosa, es preveu impossible; i 2) com ja hem vist en parlar de microdades, els mètodes basats a eliminar informació destrueixen de manera significativa la utilitat de les dades protegides.

Per solucionar el primer problema, s'han proposat solucions que intenten automatitzar el procés d'anonimitzar textos. En aquests casos la idea bàsica és analitzar els textos originals amb eines informàtiques de processament de llenguatge natural de manera que es puguin extreure els elements rellevants del text, per exemple, els substantius. Una vegada es tenen els elements rellevants identificats es pot procedir de diverses maneres; la més habitual i senzilla (Chakaravarthy *et al.*, 2008) és consultar els elements oposats en bases de dades per avaluar-ne el grau de confidencialitat. Per exemple, en un document mèdic, primer eliminaríem els noms de persones, després qualsevol tipus de número, i finalment podríem eliminar tots els substantius que coincidissin amb noms de malalties, tractaments i símptomes utilitzant una base de dades especialitzada. Altres opcions en la literatura es basen a avaluar la quantitat d'informació que cada element rellevant del text proporciona i eliminar els que són massa informatius pel risc de revelació que puguin tenir (Sánchez *et al.*, 2013).

**Lectura recomanada**

**Chakaravarthy, V. T.; Gupta, H.; Roy, P. *et al.*** (2008). «Efficient techniques for document sanitization». *Proceedings of the ACM Conf. Information and Knowledge Management* (pàg. 843-852).

**Lectura recomanada**

**Sánchez, D.; Batet, M.; Viejo, A.** (2013). «Automatic general-purpose sanitization of textual documents». *IEEE Transactions on Information Forensics and Security* (vol. 8, núm. 6, pàg. 853-862).

El problema principal d'aquestes eines automàtiques és que el llenguatge és ambigu, pot contenir errors ortogràfics i està viu (cada any el vocabulari que usem augmenta amb nous conceptes). Com a resultat d'això, pot ser difícil per a un programari detectar de manera efectiva, primer, si una part d'un text és rellevant o no i, segon, si aquesta part és perillosa o no per a la privadesa d'algun individu. Per exemple, pot ser senzill per a un programari trobar el nom de malaltia «HIV» en un text i eliminar-la, però si el text parla també dels símptomes d'aquesta malaltia i el programari no els elimina per considerar-los innocus un atacant amb un cert coneixement que llegeixi el text resultant anonimitzat pot acabar inferint que tracta sobre «HIV».

Respecte al problema de la informació que es perd en eliminar dades, en la literatura s'ha considerat usar solament l'eliminació per als identificadors directes, mentre que la resta dels elements textuals (que podrien actuar com a quasiidentificadors i/o atributs confidencials) es protegeixen mitjançant generalització a semblança del que es feia amb les microdades. En aquest cas la idea bàsica és tenir jerarquies de generalització o especialització prou àmplies per a abastar tots els conceptes del llenguatge (posat que un text lliure pot tractar qualsevol tema) o almenys els conceptes que tractaran en la tipologia de documents que volem anonimitzar (si els documents són mèdics, una jerarquia de conceptes mèdics podria ser suficient). El procés de generalitzar les dades textuals (en lloc d'eliminar-les) per retenir la major quantitat d'informació possible es denomina *sanititzar documents*.

# 8. Integració de la privadesa en el desenvolupament de productes tecnològics

En aquest apartat detallarem primer els principis relatius al tractament de les dades personals que han de complir els responsables d'aquest tractament i, per tant, tot nou producte que es vulgui desenvolupar i que treballi amb dades personals. A partir d'aquests principis introduirem una sèrie de conceptes que n'emanen directament, com la protecció de dades des del disseny i, per defecte, les tecnologies garants de la privacitat (*privacy enhancing technologies*), i les AIPD.

## 8.1. Principis relatius al tractament de les dades personals

**Lectura recomanada**

**Agencia Española de Protección de Datos** (2019). *Protección de datos: guía para el ciudadano* [en línia]. <https://www.aepd.es/media/guias/guia-ciudadano.pdf>

La normativa actual aplicable a la protecció de dades personals configura una sèrie de principis que han de ser respectats quan es produeixi el tractament de les dades. D'aquesta manera, qualsevol producte que tracti amb dades personals i, per tant, hagi de prendre mesures per a protegir la privadesa dels individus hauria de complir els principis següents recollits en l'article 5 RGPD:

- Principi de licitud, lleialtat i transparència: quan es recol·lecten dades personals han de ser tractades de manera lícita, lleial i transparent. De conformitat amb aquest principi, s'ha de proporcionar tota la informació necessària sobre l'objecte i les finalitats del tractament, les seves conseqüències i els possibles riscos per a l'interessat, tant si les dades han estat recol·lectades directament del propietari com si han estat cedides per una tercera entitat.

- Principi de limitació de la finalitat: les dades personals es recol·lecten per a unes finalitats determinades, explícites i legítimes. De conformitat amb aquest principi, la finalitat del tractament de les dades personals ha d'estar definida clarament i permesa per l'ordenament jurídic.

- Principi de minimització de dades: les dades personals recol·lectades s'han de limitar al mínim necessari en relació amb les finalitats per a les quals són tractades. De conformitat amb aquest principi, no és possible recaptar i guardar o tractar dades simplement per si poguessin ser útils en un futur.

- Principi d'exactitud: les dades personals emmagatzemades han de ser exactes i actuals. De conformitat amb aquest principi, s'han de proporcionar mesures per a poder actualitzar o suprimir les dades.

- Principi del termini de conservació: les dades personals emmagatzemades s'han de mantenir pel termini de temps mínim necessari per a complir les seves finalitats. De conformitat amb aquest principi, la conservació de

dades s'ha de limitar a les finalitats per les quals s'han recaptat. Una vegada complertes aquestes finalitats, les dades han de ser esborrades o almenys desproveïdes de tot element que permeti identificar els interessats.

- Principi d'integritat i seguretat: les dades personals han de ser tractades de manera que se'n garanteixi l'adequada seguretat, incloent la protecció contra el tractament no autoritzat o il·lícit i contra la pèrdua, destrucció o dany accidental, amb aplicació de les mesures tècniques i d'organització apropiades. De conformitat amb aquest principi, les entitats que tractin dades personals han d'actuar proactivament amb l'objectiu de protegir-les enfront de qualsevol risc que n'amenaci la seguretat. En aquest sentit les tecnologies garants de la privacitat són mètodes que ajuden a mitigar les amenaces de seguretat i protegir les dades dels individus.

- Principi de responsabilitat proactiva: els responsables i encarregats del tractament han de complir els principis anteriors i ser capaços de demostrar aquest compliment. De conformitat amb aquest principi, qualsevol producte que tracti amb dades personals ha d'aplicar els principis addicionals de protecció de dades des del disseny i protecció de dades per defecte. En la literatura aquests principis també es coneixen com a *privacy by design* i *privacy by default*.

### 8.2. Protecció de dades des del disseny i per defecte

Tal com indica l'Agència Espanyola de Protecció de Dades, en el RGPD es fa referència a dos principis per a implementar efectivament la responsabilitat proactiva, que són els de protecció de dades des del disseny i protecció de dades per defecte (art. 25 RGPD).

**Lectura recomanada**

**Agencia Española de Protección de Datos** (2019). *Medidas de protección de datos desde el diseño y por defecto* [en línia]. <https://www.aepd.es/reglamento/compliment/privadesa-per-defecte.html>

El principi de protecció de dades des del disseny té com a objectiu que la protecció de dades estigui present des de l'inici de la concepció d'un projecte (això és, l'etapa de disseny). Aquesta línia d'actuació s'ha de traduir en la implementació de les mesures tècniques i organitzatives necessàries per a aplicar de manera efectiva els principis de protecció de dades que garanteixin el tractament correcte de les dades personals.

Per exemple, aquesta línia d'actuació en una suposada botiga en línia d'aplicacions per a telèfons intel·ligents ens portaria a dissenyar el programari a càrrec de les operacions de compra de manera que apliqui l'anonimització de les dades personals dels clients (utilitzant alguna de les tècniques que hem parlat en aquest document, per exemple, *k*-Anonimitat basada en generalització i eliminació) des del moment que fan les compres, de manera que davant qualsevol ús posterior (autoritzat o no) de les dades adquirides, aquestes ja estiguessin correctament protegides.

Un punt important per tenir en compte sobre el desenvolupament de productes que comportin tasques de tractar dades personals és la necessitat de demostrar que aquests productes s'han desenvolupat tenint en compte la protecció de dades des del disseny. La pedra angular d'aquesta demostració és l'Avaluació d'Impacte en la Protecció de Dades (AIPD), una eina que analitza les activitats de tractament de dades previstes, els seus riscos i de la qual s'obté un informe amb les mesures que s'han d'aplicar per a poder garantir la protecció de les dades.

**Lectura recomanada**

**Agencia Española de Protección de Datos** (2019). *Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD* [en línia]. <https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf>

El principi de protecció de dades per defecte es refereix al fet que solament s'han d'adquirir, tractar i emmagatzemar les dades personals que siguin estrictament necessàries per a les finalitats del producte desenvolupat. Com en el cas de la privadesa des del disseny, l'aplicació de privadesa per defecte es tradueix en la implantació de mesures tècniques i organitzatives que permetin actuar en les operacions de tractament de dades següents tenint en compte els principis comentats anteriorment, que han de ser complerts:

- Recollida de dades: s'ha de recaptar la mínima quantitat de dades personals possibles en funció dels productes i serveis seleccionats per l'usuari.

- Tractament de les dades: qualsevol procés que utilitzi dades personals ha d'accedir a les mínimes dades possibles necessàries per a complir la seva tasca.

- Conservació: s'ha d'implementar una política de conservació de dades que permeti eliminar les dades que no siguin estrictament necessàries.

- Accessibilitat: s'ha de limitar l'accés a les dades personals per part de tercers.

### 8.3. *Privacy enhancing technologies* (PET)

Les *privacy enhancing technologies* (PET) són tecnologies de millora de la privadesa l'objectiu de les quals és protegir la privadesa dels usuaris de tecnologia; això és, són tecnologies que protegeixen la confidencialitat de les dades dels individus.

**Lectura recomanada**

**Wang, Y.; Kobsa, A.** (2008). *Privacy-enhancing technologies: handbook of research on social and organizational liabilities in information security* (pàg. 352-375).

Aquesta és una categoria d'eines molt general i, per tant, engloba totes les tecnologies que s'han creat per protegir la privadesa de les persones de molt diverses maneres. Per exemple, hi ha PET que anonimitzen la navegació web dels individus, PET que xifren les comunicacions entre entitats perquè un atacant extern no pugui accedir a les transmissions o modificar-les d'alguna manera, PET que proporcionen control als usuaris d'una xarxa social sobre qui pot accedir a certes dades personals o missatges, o PET que ofusquen la localització física d'una persona de manera que un servei basat en localització no pugui conèixer la seva localització exacta en un determinat instant de temps.

Les PET, per tant, engloben moltes tecnologies diferents que protegeixen la privadesa dels individus de diferents maneres i poden ser utilitzades per diferents actors durant l'execució d'un servei. Tal com hem dit, un usuari de serveis basats en localització, per exemple, podria usar una PET controlada per ell mateix perquè l'entitat que ofereix el servei no conegui mai la seva localització exacta, o podria ser aquesta entitat la que utilitzés una PET per a protegir les dades de localització que obté dels seus usuaris, o l'usuari i l'entitat podrien usar una PET per a comunicar-se de manera xifrada i segura entre ells evitant l'acció de qualsevol atacant extern.

És complicat classificar la gran diversitat de les PET existents en la literatura o destacar unes solucions sobre unes altres. A continuació descriurem algunes tipologies de PET per la seva rellevància i quotidianitat, però no pretenem fer una classificació formal ni indicar que aquestes siguin les PET més rellevants.

- Protecció de comunicacions: en les comunicacions entre dues entitats en entorns insegurs, per exemple, quan un usuari vol comprar un ítem en una botiga en línia i ha de proporcionar les seves dades bancàries, és habitual utilitzar la tecnologia TLS/SSL per a xifrar les comunicacions entre l'explorador web i el servidor web.

- Anonimització de la navegació web: cada vegada que un usuari accedeix a una pàgina web envia al servidor corresponent una gran quantitat de dades, les quals inclouen les conegudes galetes però també la configuració de l'explorador web utilitzat. D'aquesta manera, la navegació web deixa un rastre que permet fer el seguiment dels individus. Una eina famosa per a anonimitzar la navegació web és la xarxa TOR. Aquesta xarxa fa d'intermediari entre l'explorador web i el servidor web que ofereix la pàgina web, de manera que, per a sol·licitar la pàgina web, la xarxa TOR crea una combinació de màquines situades a la xarxa que seran les que demanaran finalment la pàgina web al servidor en lloc de l'usuari. Com a resultat d'això, el servidor web mai no sabrà qui va sol·licitar la pàgina web en realitat.

- Sistemes de gestió de la identitat: cada vegada que un individu vol usar un servei és normal que hagi d'autenticar-se al servidor que l'ofereix. Un procés d'autenticació implica que el servidor ha de conèixer certes dades privades de l'individu (per exemple, una contrasenya), de manera que l'individu pugui demostrar la seva identitat revelant dades que hauria de conèixer solament ell. Com que en l'actualitat hi ha una gran quantitat de serveis tecnològics, el fet que totes les entitats que els ofereixen haguessin de conèixer dades privades dels individus podria ser un problema important de privadesa i seguretat. Per a evitar això, hi ha tecnologies com OpenID, que permet que compartim simplement dades privades amb una única entitat i que aquesta ens «representi» davant de totes les altres.

**Lectura recomanada**

Sobre el procés d'anonimització:

**Sánchez, D.; Batet, M.; Viejo, A.** (2013). «Automatic general-purpose sanitization of textual documents». *IEEE Transactions on Information Forensics and Security* (vol. 8, núm. 6, pàg. 853-862).

- Sistemes de control d'accés: els sistemes de control d'accés permeten als individus definir exactament, mitjançant polítiques d'accés, quina entitat pot actuar (llegir, usar, esborrar, etc.) sobre un cert recurs (text, imatge, aplicació, etc.). Això és molt habitual, per exemple, en les xarxes socials, on un usuari pot publicar alguna cosa i fer que solament els seus amics puguin llegir-la o comentar-la, o pot fer que un cert recurs publicat sigui accessible per a tothom. D'aquesta manera, la configuració de privadesa d'una xarxa social és una PET, encara que molt senzilla. Sistemes de control d'accés més complexos i amb més funcionalitats són, per exemple, els basats en ABAC (això és, control d'accés basat en atributs), aplicats mitjançant una arquitectura XACML amb el respectiu llenguatge de polítiques d'accés.

- Anonimització de microdades: hem dedicat la major part d'aquesta documentació a explicar com es protegeix la privadesa dels individus en entorns de publicació de dades. En aquest sentit, el conjunt de tècniques necessàries per a generar una taula de microdades protegida sota *k*-Anonimitat són PET.

- Transferències de dades anònimes mitjançant cadena de blocs: en l'actualitat és molt habitual que les transferències d'informació important entre dos individus requereixin una tercera entitat, teòricament de confiança, que doni fe de la transacció que té lloc i en gestioni els efectes. Parlem, per exemple, de transaccions de diners electrònics entre un comprador i una botiga en línia, on hi ha un banc que gestiona la transferència de diners d'un compte a un altre en el seu entorn segur, o d'algun tipus de contracte legal amb certes obligacions per a les dues parts, que ha de ser verificat per un notari. L'existència d'aquesta tercera entitat que ho sap tot i ho gestiona tot comporta per si mateixa un problema de privadesa. La PET que soluciona aquest problema és la cadena de blocs.
  La cadena de blocs és una base de dades de transferències d'informació distribuïda totalment on els individus són els qui hi «escriuen» a sobre i verifiquen que el que uns altres han escrit sigui correcte. Així, doncs, en aquest entorn no hi ha una entitat central que ho sap tot i ho gestiona tot, sino una comunitat d'individus que s'han donat unes regles comunes d'actuació i en la qual tot funcionarà correctament mentre la majoria dels individus es comporti de manera honesta.
  La cadena de blocs per si mateixa no és més que una mena de «pissarra pública» on els individus anoten totes les transaccions que s'han fet entre ells des de l'inici del sistema. Un exemple de transacció en el cas de la substitució dels bancs és «Individu 1234 transfereix deu monedes a Individu 2223». Perquè la comunitat doni per bona aquesta transacció, el que farà serà comprovar a la pissarra (l'històric de transaccions fetes des del primer dia) que l'individu «1234» té realment deu monedes; per a això, la comunitat comprovarà que entre les transferències que ha rebut i les que ha enviat encara li queden deu monedes. Si «1234» té aquestes 10 monedes, la comunitat donarà la nova transferència per bona i, a partir d'aquest

moment, l'individu «2223» podrà usar aquestes monedes per a fer altres noves transferències.

La «pissarra» de què parlem té tot un conjunt de tecnologies criptogràfiques perquè les transferències es facin de manera segura i confiable (la qual cosa inclou l'ús de signatures digitals). Un factor interessant amb vista a la privadesa és que els individus no usen la seva identitat real sinó un identificador que es genera a partir d'unes claus criptogràfiques i que els individus poden canviar quan vulguin. D'aquesta manera, un observador no pot conèixer la identitat real de l'individu «1234». No obstant això, la privadesa oferta d'aquesta manera pot trencar-se fàcilment si en algun moment hem de vincular la identitat real amb l'identificador utilitzat en la cadena de blocs, per exemple, si una compra requereix que ens identifiquem.

Finalment, cal destacar que la finalitat de la cadena de blocs és aconseguir que una comunitat d'individus iguals pugui gestionar transferències entre ells ocultant les seves identitats reals. El contingut de les transferències no es xifra, ja que tota la comunitat ha de poder veure-les i verificar-ne la validesa; sí que s'aplica criptografia per garantir-ne la integritat i autenticitat, això és, solament el propietari de les claus criptogràfiques necessàries pot demostrar que és l'«Individu 1234» i ningú no pot alterar una de les transferències que apareixen en la pissarra pública.

### 8.4. Avaluació d'impacte en la protecció de dades (AIPD)

L'aplicació del principi de protecció de dades des del disseny requereix que el responsable del tractament de dades personals consideri des de l'inici, en la fase de disseny, les accions preventives suficients per a poder identificar, avaluar i tractar els riscos associats al tractament de dades personals i, així, poder assegurar els principis de protecció de les dades amb la garantia dels drets i llibertats dels interessats.

Per a cobrir aquest requeriment, tenim l'eina Avaluació d'Impacte en la Protecció de Dades Personals (AIPD), la qual permet avaluar de manera anticipada quins són els riscos a què estan exposades les dades personals en funció de les activitats que es duran a terme amb elles i establir una resposta a aquests riscos adoptant les mesures de protecció necessàries per a reduir-los fins a un nivell de risc acceptable.

**Lectura recomanada**

**Agencia Española de Protección de Datos** (AEPD) (2019). *Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD* [en línia]. <https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf>

El procés per a fer una AIPD consta de tres seccions, que es desglossen al seu torn en diferents tasques:

1) Context
a) Descriure el cicle de vida de les dades.
b) Analitzar la necessitat i proporcionalitat del tractament.

2) Gestió de riscos
a) Identificar amenaces i riscos.

b) Avaluar els riscos.
c) Tractar els riscos.

3) Conclusió
a) Pla d'acció i informe de conclusions.

El cicle de vida de les dades es divideix en les etapes següents: captura de dades, emmagatzematge, ús o tractament, cessió a tercers i destrucció. En aquesta tasca de l'AIPD, s'ha de poder respondre les preguntes següents per a cada etapa del cicle de vida:

- Qui duen a terme els rols següents: interessats, responsable del tractament, encarregat del tractament i terceres parts.
- Quins sistemes d'informació hi ha involucrats.
- Quins fluxos de dades hi ha entre els diferents sistemes d'informació i els diferents rols.
- Qui té accés a les dades i amb quina finalitat.
- Quina és la base legitimadora de les activitats de tractament: consentiment exprés, relació contractual, interès legítim, etc.

En la tasca d'analitzar la necessitat i proporcionalitat de les activitats de tractament es respondran les preguntes següents:

- Què es farà amb les dades i amb quina finalitat?
- Quines dades es tractaran?
- Són necessàries totes? Qui és l'afectat per les dades que cal tractar? Se li ha informat correctament?

Aquestes qüestions estan relacionades directament amb els principis de licitud, lleialtat i transparència; minimització de dades i limitació de la finalitat. La proporcionalitat que caldrà aplicar en el tractament de dades es basa a avaluar si la finalitat que es persegueix es pot aconseguir per altres mitjans, per exemple, utilitzant altres dades o fent ús d'altres mètodes menys invasius, com modificar altres dades que es tinguin per evitar recol·lectar-ne de noves.

En la tasca d'identificar amenaces i riscos, s'identifiquen primer les amenaces tenint en compte les operacions que es fan en tot el cicle de vida de les dades i la classificació d'amenaces segons la seva tipologia: 1) accés il·legítim a dades, 2) modificació no autoritzada de les dades, i 3) eliminació de les dades. D'aquesta manera, en l'etapa d'«emmagatzematge» del cicle de vida de les dades podríem tenir com una amenaça del tipus «accés il·legítim a dades» un «atac intencionat fet per un *hacker*» o «accés intencionat per part de personal no autoritzat», o podríem tenir com a amenaça del tipus «eliminació de dades» un «error humà que provoqui esborrament de dades».

Una vegada s'identifiquen les amenaces, aquestes es relacionen amb riscos i el seu possible impacte. Per exemple, l'amenaça «accés intencionat per part de personal no autoritzat» en l'etapa de cicle de vida «emmagatzematge» pot produir com a risc la «vulneració dels drets i llibertats» dels propietaris de les dades, i l'impacte seria «dany moral, físic o material».

La tasca d'identificar amenaces, riscos i el seu impacte es pot procedimentar seguint els llistats de riscos associats al compliment normatiu que ofereix l'Agència Espanyola de Protecció de Dades.

La tasca d'*avaluar els riscos* requereix estimar la probabilitat que el risc es materialitzi i estimar el nivell d'impacte en cas que es materialitzi. La probabilitat de risc i el nivell d'impacte es classifiquen en quatre nivells numèrics: probabilitat/impacte menyspreable (valor 1), probabilitat/impacte limitat (valor 2), probabilitat/impacte significatiu (valor 3) i probabilitat/impacte màxim (valor 4). Amb els valors estimats, es pot calcular el nivell de risc de l'amenaça (anomenat **risc inherent**) multiplicant el valor de probabilitat de risc i el valor d'impacte; segons el resultat numèric obtingut, el nivell de risc de l'amenaça es classificarà en quatre nivells: baix (1-2), mitjà (3-6), alt (7-9) i molt alt (10-16).

En la tasca de tractar els riscos es definiran les mesures necessàries per a tractar les amenaces amb nivells de risc per sobre de l'acceptable. Hi ha tres mesures principals per a tractar el risc: reduir-lo amb mesures de control; transferir-lo a una altra organització, per exemple, contractant una asseguradora que afronti les possibles conseqüències materials; o anul·lar-lo completament, la qual cosa implica no fer el tractament o ús de dades al qual l'amenaça està vinculada.

Entre les mesures de control que busquen reduir el risc hi ha: 1) mesures organitzatives, per exemple, definició de procediments per a exercir els drets dels interessats; 2) mesures legals, per exemple, clàusules per a recollir consentiments expressos; i 3) mesures tècniques, que són les que vetllen per la seguretat dels actius d'informació, això és, les tecnologies garants de la privacitat, per exemple, anonimització sota *k*-Anonimitat, protegir comunicacions sota SSL/TLS, etc.

Després de l'aplicació de les mesures de control, s'ha de calcular de nou el nivell de risc de l'amenaça en qüestió (anomenat **risc residual**) per a poder avaluar i documentar de quina manera s'ha reduït el risc inherent.

La tasca final correspon al pla d'acció i informe de conclusions. En aquesta etapa es documentarà el resultat de l'AIPD juntament amb el pla d'acció que inclogui les mesures de control que caldrà implantar per a gestionar els riscos identificats. Si el resultat de l'AIPD és no favorable, s'ha d'analitzar la possibilitat d'incloure mesures de control addicionals que permetin reduir l'exposició

al risc fins a un nivell acceptable. Si el resultat és favorable, l'activitat de tractament o ús de les dades personals es pot dur a terme sempre que les mesures de control incloses en el pla d'acció hagin estat implantades.

Cal destacar que, per a complir el principi de protecció de dades des del disseny, és necessari considerar el pla d'acció resultant d'aquesta tasca durant la fase de definició del nou producte tecnològic que ha d'utilitzar dades personals.

Com a nota final, per a detalls específics sobre com fer correctament una AIPD, el lector hauria de consultar la «Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD» de l'Agència Espanyola de Protecció de Dades.

**Lectura recomanada**

**Agencia Española de Protección de Datos** (AEPD) (2019). *Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD* [en línia]. <https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf>

## Resum

En aquest mòdul hem fet una descripció completa de les amenaces a la privadesa i els mecanismes de protecció vinculats a la publicació de microdades principalment però també a la publicació d'altres tipus de dades, com les transaccionals, de moviment d'objectes o textuals. També hem explicat com es té en compte la protecció de la privadesa en el desenvolupament de nous productes tecnològics que tracten amb dades personals, explicant conceptes rellevants sobre aquest tema, com la privadesa des del disseny i la privadesa per defecte.

En el primer apartat hem parlat dels tipus de dades habituals que s'utilitzen en publicar informació en entorns oberts com internet.

En el segon apartat hem parlat dels dos objectius principals a l'hora de proporcionar privadesa en la publicació de dades: l'anonimat i la confidencialitat. Ens hem centrat en la diferència entre dades anonimitzades i dades pseudonimitzades. I finalment hem explicat quin és el problema que s'ha de resoldre en fer un procés d'anonimització de dades.

En el tercer apartat hem descrit el risc de revelació d'identitat i el risc de revelació d'atribut, riscos que defineixen directament l'estratègia de protecció a seguir per minimitzar-los.

En el quart apartat hem explicat els diferents mètodes d'anonimització de dades distingint entre mètodes basats en pertorbació, no-pertorbació i generació de dades sintètiques.

En el cinquè apartat hem parlat sobre la importància de preservar la utilitat de les dades protegides i hem donat explicacions sobre el nivell de retenció de la utilitat obtingut segons el mètode d'anonimització utilitzat.

En el sisè apartat hem explicat què és un model de privadesa i hem detallat el model de *k*-Anonimitat, el més cèlebre en la literatura, i les seves extensions.

En el setè apartat ens hem centrat en l'anonimització de dades transaccionals, de moviment d'objectes i textuals; els dos primers són similars a les microdades però tenen certes peculiaritats a les quals cal fer atenció. El cas de les dades textuals és bastant més diferent, encara que al final les mesures de protecció aplicades per a aquest tipus de dades són similars.

Finalment, en el vuitè apartat hem explicat la integració de la privadesa en el desenvolupament de productes tecnològics partint dels principis relatius al tractament de dades personals establerts pel Reglament general de protecció

de dades (RGPD). En aquest apartat hem parlat de conceptes rellevants, com la protecció de dades des del disseny i per defecte, i les tecnologies garants de la privacitat, i, finalment, hem explicat succintament com es fa una avaluació d'impacte en la protecció de dades (AIPD), que és una eina que ens permet demostrar documentalment l'aplicació de la privadesa des del disseny en el desenvolupament de tecnologies que tractin amb dades personals.

# Bibliografia

**Agencia Española de Protección de Datos (AEPD)** (2019). *Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD*. [en línia]. <https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf>

**Agencia Española de Protección de Datos (AEPD)** (2019). *La k-Anonimidad como medida de la privacidad.* [en línia]. <https://www.aepd.es/media/notas-tecnicas/nota-tecnica-kanonimidad.pdf>

**Agencia Española de Protección de Datos (AEPD)** (2019). *Medidas de protección de datos desde el diseño y por defecto*. [en línia]. <https://www.aepd.es/reglamento/cumplimiento/privacidad-por-defecto.html>

**Agencia Española de Protección de Datos (AEPD)** (2019). *Protección de datos: guía para el ciudadano.* [en línia]. <https://www.aepd.es/media/guias/guia-ciudadano.pdf>

**Barbaro M.; Zeller T.** (2006). «A face is exposed for AOL searcher no. 4417749». *New York Times* (agost).

**Benjamin, C. M. F.; Ke Wang, R. C.; Philip, S. Yu.** (2010). «Privacy-preserving data publishing: a survey of recent developments». *ACM Computing Surveys* (vol. 42, núm. 4, art. 14).

**Chakaravarthy, V. T.; Gupta, H.; Roy, P.; Mohania, M.** (2008). «Efficient techniques for document sanitization». *Proceedings of the ACM Conf. Information and Knowledge Management* (pàg. 843-852).

**Dalenius, T.; Reiss, S. P.** (1978). «Data-swapping: a technique for disclosure control» *Proceedings of the ASA Section on Survey Research Methods* (pàg. 191-194).

**Defays, D.; Anwar, M. N.** (1998). «Masking microdata using micro-aggregation». *Journal of Official Statistics* (vol. 14, núm. 4, pàg. 449-461).

**Department of Health and Human Services, Office of the Secretary.** (2000). *The Health Insurance Portability and Accountability Act of 1996*. Tech. Rep. Federal Register 65 FR 82462.

**Domingo-Ferrer, J.; Sánchez, D.; Soria-Comas, J.** (2016). *Database anonymization: privacy models, data utility, and microaggregation-based inter-model connections*. Morgan & Claypool Publishers.

**Greenberg, B.** (1996). *Rank swapping for masking ordinal microdata*. Washington DC: U.S. Bureau of the Census.

**Hundepool, A.; Domingo-Ferrer, J.; Franconi, L. *et al.*** (2012). *Statistical Disclosure Control*. Wiley.

**Latanya, S.** (2000). «Uniqueness of simple demographics in the U.S. population». *LIDAP-WP4*. Pittsburgh PA: Carnegie Mellon University, Laboratory for International Data Privacy.

**Li, N.; Li, T.; Venkatasubramanian, S.** (2007). «*t*-closeness: privacy beyond *k*-anonymity and *l*-diversity». *ICDE* (pàg. 106-115). IEEE.

**Machanavajjhala, A.; Kifer, D.; Gehrke, J.; Venkitasubramaniam, M.** (2007). «*l*-diversity: privacy beyond *k*-anonymity». *ACM Transactions on Knowledge Discovery from Data* (vol. 1, núm. 1).

**Parlamento Europeo** (2016). *Reglamento (UE) 2016/679, general de protección de datos (RGPD).* [en línia]. <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

**Rodríguez, M.** (2017). *Semantic perturbative privacy-preserving methods for nominal data*. Tesi doctoral. Universitat Rovira i Virgili.

**Rubin, D. B.** (1993). «Discussion: statistical disclosure limitation». *Journal of Official Statistics* (vol. 9, pàg. 462-468).

**Rubner, Y.; Tomasi, C.; Guibas, L. J.** (2000). «The earth mover's distance as a metric for image retrieval». *International Journal of Computer Vision* (vol 40, núm. 2, pàg. 99-121).

**Samarati, P.; Latanya, S.** (1998). «Protecting privacy when disclosing information: *k*-anonymityand its enforcement through generalization and suppression». *Informe tècnic* . SRI International.

**Sánchez, D.; Batet, M.; Viejo, A.** (2013). «Automatic general-purpose sanitization of textual documents». *IEEE Transactions on Information Forensics and Security* (vol. 8, núm. 6, pàg. 853-862).

**Sánchez, D.; Viejo, A.** (2017). «Personalized privacy in open data sharing scenarios». *Online Information Review* (vol. 41, núm. 3).

**Soria-Comas, J.; Domingo-Ferrer, J.** (2015). «Big data privacy: challenges to privacy principles and models». *Data Science and Engineering* (pàg. 1-8).

**Terrovitis M.; Mamoulis N.; Kalnis, P.** (2008). «Privacy-preserving anonymization of set-valued data». *Proceedings of the VLDB Endowment* (vol. 1, pàg. 115-125).

**US Federal Trade Commission.** (2014). *Data brokers, a call for transparency and accountability.*

**Wang, Y.; Kobsa, A.** (2008). *Privacy-enhancing technologies: handbook of research on social and organizational liabilities in information security*(pàg. 352-375).

**Warren; Brandeis** (1890). «The Right to Privacy». *Harvard Law Review* (vol. 193).

**Willenborg, L.; De Waal T.** (2001). *Elements of statistical disclosure control*. Nova York: Springer-Verlag.