Privadesa en temps de megadades: entre el nihilisme i el fonamentalisme

Discurs de presentació de Josep Domingo-Ferrer com a membre numerari de la Secció de Ciències i Tecnologia, llegit el dia 21 de novembre de 2016

Institut d'Estudis Catalans

SECCIÓ DE CIÈNCIES I TECNOLOGIA

Privadesa en temps de megadades: entre el nihilisme i el fonamentalisme

Privadesa en temps de megadades: entre el nihilisme i el fonamentalisme

Discurs de presentació de Josep Domingo-Ferrer com a membre numerari de la Secció de Ciències i Tecnologia, llegit el dia 21 de novembre de 2016

Barcelona, 2016

Institut d'Estudis Catalans

SECCIÓ DE CIÈNCIES I TECNOLOGIA

Biblioteca de Catalunya. Dades CIP

Domingo-Ferrer, Josep, 1965-
Privadesa en temps de megadades : entre el nihilisme i el fonamentalisme
Bibliografia
ISBN 9788499653242
I. Institut d'Estudis Catalans. Secció de Ciències i Tecnologia II. Títol
1. Dades massives 2. Protecció de dades 3. Dret a la intimitat
004.6.056.5:342.737/.738

Carrer del Carme, 47. 08001 Barcelona

Primera edició: novembre del 2016

Text revisat lingüísticament per la Unitat de Correcció del Servei Editorial de l'IEC

Disseny de la coberta: Azcunce | Ventura

Compost per fotocomposició gama, s. l.
Imprès a Open Print, SL

ISBN: 978-84-9965-324-2
Dipòsit Legal: B 21612-2016

1. Introducció

Les megadades han esdevingut una realitat amb el canvi de mil·lenni. Gairebé qualsevol activitat humana deixa un rastre digital que algú recull i emmagatzema (sensors de la Internet de les coses, aplicacions socials, comunicació màquina-màquina, vídeo mòbil, etc.). Com a resultat, és possible disposar de dades de moltes fonts independents, que poden fusionar-se i analitzar-se per generar coneixement. Les megadades es diferencien dels fitxers de dades tradicionals en diversos aspectes:

— *Volum*. Es poden arribar a manejar volums de zettaoctets (10^{21} octets). S'estima que Facebook tot sol ingereix 500 teraoctets de dades al dia (500×10^{12} octets). Segons IBM (Meeker, 2014), l'any 2013 es van generar 4 zettaoctets a tot el món. S'estima que el 2020 hi haurà 50.000 milions de sensors connectats a Internet, que produiran encara moltes més dades.

— *Velocitat*. Hi ha un nombre creixent de fluxos continus de dades provinents de sensors o de xarxes socials (per exemple, els fluxos de Twitter). Hom pot capturar dades en línia de milions d'esdeveniments per segon i els sensors generen fitxers de registre immensos. Amb aquestes dades, els algorismes d'anàlisi poden fornir tendències del mercat i predir el comportament de les persones en qüestió de microsegons (de fet, els robots inversors ja fa temps que dominen els mercats borsaris i els inestabilitzen).

— *Varietat*. Les dades vénen de moltes menes diferents de sensors i de sistemes, en diferents formats. Trobem dades numèriques, categòriques, geoespacials, 3D, àudios, vídeos, textos no estructurats (incloent-hi fitxers de registre i xarxes socials), etc.

Els grans volums de dades que es manegen han desbordat l'emmagatzematge estructurat tradicional i han obligat a crear noves tecnologies, com Hadoop, NoSQL, MapReduce, etc. (Dean i Ghemawat, 2008). Al mateix temps, la varietat i el volum de la informació disponible han donat pas a anàlisis molt sofisticades que ni tan sols s'intuïen anys enrere. L'anàlisi de dades ja no és només qüestió de descriure les dades o de provar-hi hipòtesis, sinó també d'extreure'n coneixement que hom no tenia prèviament. Estem passant d'una estadística tradicional que intentava inferir veritats poblacionals a partir de mostres comparativament i necessàriament petites a una anomenada *ciència de dades* (*data science*) que dóna per descomptat l'accés a pràcticament totes les dades de la població d'interès.

Tot i que les megadades són un recurs valuosíssim en molts camps, tenen un efecte secundari certament important: com més va més amenacen la privadesa dels subjectes les dades dels quals es recullen i s'analitzen (sovint sense que ells en tinguin esment). El cas que s'explica a Duhigg (2012) és força il·lustratiu. Target, una cadena de venda al detall, va crear un model de predicció de l'embaràs. L'objectiu era enviar vals de descompte de diversos productes relacionats amb els nadons tan aviat com fos possible, per tal de formar hàbits de compra de llarga durada que afavorissin Target. Al cap d'un quant temps, un pare es va queixar que sa filla, encara alumna d'institut, havia rebut vals de descompte per a roba de nadó; demanava si la cadena estava animant sa filla a quedar-se embarassada. Més tard, es va descobrir que la noia realment estava embarassada però que son pare encara no ho sabia.

En un escenari i a una escala diferents, el risc de revelació ha estat una preocupació constant de les comunitats estadística i informàtica, que han proposat diversos mètodes per limitar-lo. El control de la revelació estadística o secret estadístic (conegut per les seves sigles angleses SDC, de *statistical disclosure control*, Hundepool *et al.*, 2012) cerca de permetre inferències útils sobre subpoblacions a partir d'un fitxer de dades, tot i que preserva la privadesa dels subjectes als quals corresponen les dades del fitxer. Els investigadors hem dissenyat un bon nombre de tècniques per limitar el risc de revelació en la publicació de dades referents a subjectes individuals, les anomenades *microdades*. Aquestes tècniques tenen el tret comú de guardar en secret les dades originals i substituir-les per una versió modificada, que s'anomena *versió anonimitzada*. En els darrers vint anys, d'altra banda, també s'han proposat diversos *models de privadesa*. En comptes de determinar la transformació concreta que cal aplicar a les dades originals, un model de privadesa especifica una condició que, si és satisfeta pel fitxer anonimitzat, garanteix que el risc de revelació està sota control. Els models de privadesa normalment tenen un o diversos paràmetres que determinen quant de risc de revelació és acceptable. Els models existents han estat pensats per a un sol fitxer de dades, però en un escenari de megadades tenen força insuficiències.

La resta d'aquest discurs té l'estructura següent. A l'apartat 2, examinarem el conflicte entre les megadades i els requisits ètics i legals de la gestió de dades privades. A l'apartat 3, exposarem la posició dels nihilistes, que sostenen que està fora de lloc voler preservar la privadesa en el món de les megadades; diuen que, com a molt, els subjectes poden demanar que les seves dades es facin servir a fi de bé. A l'apartat 4, presentarem la posició dels fonamentalistes, que prioritzen tant la privadesa que els seus mètodes pràcticament inutilitzen les dades des del punt de vista analític, amb la qual cosa l'anàlisi exploratòria habitual en megadades esdevé impossible. A l'apartat 5, esbossarem un «camí del mig» que transiti entre l'Escil·la del nihilisme i la Caribdis del fonamentalisme i condueixi a unes megadades que siguin raonablement útils per a l'anàlisi exploratòria i protegeixin raonablement la privadesa dels subjectes individuals; començarem identificant algunes propietats que hauria de tenir un model de privadesa per ser útil en aquest camí del mig, i després avaluarem fins a quin punt els dos models de privadesa principals compleixen aquestes propietats. Finalment, a l'apartat 6, recollirem unes conclusions i enumerarem línies de recerca que queden obertes.

2. Megadades, llei i ètica

El risc potencial per a la privadesa és un dels inconvenients més grans de les megadades. Cal tenir present que les megadades s'obtenen precisament recollint totes les dades possibles per extreure'n coneixement, possiblement amb mètodes innovadors. D'altra banda, massa sovint el subjecte de les dades (típicament un consumidor, un ciutadà, etc.) no les dóna conscientment. Més aviat, el proveïdor d'algun servei aconsegueix les dades indirectament com a resultat d'una transacció (per exemple, quan el consumidor mira o compra productes en una botiga en línia), com a retorn d'un servei gratuït (per exemple, correu electrònic o xarxes socials, etc.) o com a requisit natural d'algun servei (per exemple, un sistema de navegació GPS necessita conèixer la posició d'un individu per fornir-li informació sobre el trànsit proper al lloc on es troba).

Actualment, no hi ha una visió clara de quines són les millors estratègies per protegir la privadesa enfront de les megadades. Abans de les dades massives, hom solia aplicar els principis següents en la legislació per protegir la informació identificable personalment (IIP) (Danezis *et al.*, 2015):

— *Legalitat*. O bé cal obtenir el consentiment del subjecte, o bé el processament de les dades ha d'ésser necessari per obligació legal o contractual per als interessos vitals del subjecte o per a interessos legítims del processador compatibles amb els drets del subjecte.

— *Consentiment*. El consentiment donat pel subjecte ha d'ésser senzill, específic, informat i explícit.

— *Limitació de propòsit*. El propòsit de la recollida de les dades ha d'ésser legítim i especificat abans de la recollida.

— *Necessitat i minimització de les dades*. Només cal recollir les dades necessàries per al propòsit concret. A més, cal conservar les dades només el temps estrictament necessari per al propòsit.

— *Transparència i obertura*. Els subjectes han de rebre informació sobre la recollida i el processament de llurs dades d'una manera que puguin entendre.

— *Drets individuals*. Els subjectes haurien de tenir accés a les dades sobre ells, i també haurien de poder rectificar-les o fins i tot esborrar-les (dret a l'oblit).

— *Seguretat de la informació*. Les dades recollides s'han de protegir de l'accés, del processament i de la manipulació no autoritzats, i també de la pèrdua i de la destrucció.

— *Responsabilitat*. L'entitat que recull i processa les dades ha de poder demostrar que compleix els principis anteriors.

— *Protecció de dades per disseny i per defecte*. Cal incorporar la privadesa des del principi del disseny d'un producte o d'un servei, no pas posteriorment, com si fos un pegat.

Sense anonimització, hi ha diversos conflictes potencials entre els principis esmentats suara i el propòsit de les megadades. Pel que fa a la limitació de propòsit, sovint es fan usos secundaris de les megadades que ni tan sols es preveien en el moment de llur recollida. Quant al consentiment, és difícil d'obtenir-lo si el propòsit de la recollida de dades no és clar de bon començament. Sense limitació de propòsit ni consentiment, la legalitat és dubtosa. D'altra banda, com que les megadades s'obtenen acumulant dades per a ús potencial, són difícilment compatibles amb el principi de necessitat i minimització de dades. Quant als drets individuals, els subjectes difícilment els poden exercir, perquè no saben quines dades es guarden sobre ells i qui les guarda; per tant, se'ls fa impossible l'accés, la rectificació o l'esborrament. Finalment, la responsabilitat de qui recull i processa les dades és paper mullat: si no compleix la majoria dels principis, no pot demostrar que els compleix.

Atesos els conflictes anteriors entre les megadades i la protecció de dades, un corrent d'opinió és que, per no entorpir el desenvolupament tecnològic, la protecció de la privadesa s'hauria de limitar a usos potencialment nocius per a la privadesa. Per tant, la recollida de dades en quedaria al marge. Fins i tot, hi ha qui advoca per l'autoregulació. Aquest corrent minimalista, sobretot alimentat per les grans empreses d'Internet, s'enfronta a un corrent maximalista que sosté que les esquerdes de la privadesa comencen amb la mera recollida de dades. Certament, un cop s'han recollit les dades, sorgeixen diverses amenaces (Brookman i Hans, 2013):

— *Violació de dades*. Pot ocórrer com a resultat d'atacs informàtics o de mesures de seguretat insuficients. Com més dades es recullen, més atractives són per a un atacant.

— *Mal ús per part d'empleats* (Chen, 2010). Els empleats de l'entitat que recull, emmagatzema o processa les dades poden fer-ne un mal ús.

— *Ús secundari no desitjat*. Pot passar que l'entitat que processa les dades en faci usos que el subjecte no volia. Per exemple, les dades sanitàries d'un subjecte contrari als anticonceptius poden fer-se servir per fer recerca sobre nous anticonceptius.

— *Canvis en les pràctiques empresarials*. Les polítiques que impedeixen a una empresa de fer servir les dades en perjudici dels interessos dels subjectes poden canviar (per exemple, recentment WhatsApp ha decidit unilateralment de compartir els números de mòbil dels seus usuaris amb Facebook, la seva propietària).

— *Accés governamental sense les garanties legals degudes* (Solove, 2011). Tal com s'ha vist arran de les revelacions de Snowden, l'Agència Nacional de Seguretat dels EUA accedia de manera il·legal (o, si més no, alegal) a les dades dels usuaris de les grans empreses d'Internet.

Les tècniques d'anonimització són una possible solució per superar els conflictes entre els principis de protecció de dades i les megadades. Com que els principis anteriors es refereixen a IIP, un cop les dades han estat anonimitzades, es pot pensar que ja no són IIP i que ja no necessiten protecció. Tanmateix, les tècniques d'anonimització presenten dificultats quan s'apliquen a les megadades. D'una banda, massa poca anonimització (per exemple, només suprimir els identificadors directes dels subjectes) pot ser insuficient per garantir que no es podran reidentificar els subjectes (Barbaro i Zeller, 2006; Hansell, 2006). Amb les megadades, això és especialment problemàtic, perquè, a mesura que augmenten la quantitat i la varietat de les dades acumulades sobre un individu determinat, és més plausible que se'l reidentifiqui. D'altra banda, massa anonimització pot impedir d'aparellar dades sobre el mateix subjecte (o subjectes semblants) que provenen de diferents fonts, amb la qual cosa es perden molts dels beneficis potencials de les megadades.

3. Els nihilistes: amb megadades no hi pot haver privadesa

Hi ha com a mínim dos arguments per defensar la mort de la privadesa. El primer diu que cal sacrificar la privadesa totalment o parcialment en nom de la seguretat. El segon argument és menys doctrinari i més pragmàtic: consisteix a presentar la privadesa com una nosa sense la qual podríem disposar de molts més serveis i funcionalitats.

El sacrifici necessari de la privadesa a l'altar de la seguretat ha estat predicat per governs i per empreses. Pel cantó governamental, ja el 2009, l'excoordinador de seguretat i intel·ligència del Regne Unit, Sir David Omand, va avisar que «els ciutadans hauran de sacrificar llur dret a la privadesa en la lluita contra el terrorisme». L'argument és que els serveis d'intel·ligència necessiten accedir a un ventall molt ampli de dades personals, incloent-hi enregistraments telefònics, correus

electrònics, interaccions a les xarxes socials i informació de viatge. Aquest ex-alt càrrec britànic va anar més lluny i va escriure que «descobrir els secrets del proïsme implicarà trencar les regles morals de cada dia». En aquesta línia, el mes d'abril passat, el Parlament Europeu va aprovar per 461 vots a 179 que els serveis de seguretat europeus comparteixin la informació dels passatgers aeris.

Algunes empreses també s'han apuntat a la seguretat a costa de la privadesa: n'és un bon exemple la implantació de sistemes biomètrics de control d'accés en aeroports i fins i tot en llocs de seguretat tan poc crítica com gimnasos i piscines. Obligar els treballadors i, encara pitjor, els clients a fer servir llurs empremtes digitals o llur patró retinal com a contrasenya és una clara violació de la privadesa. Què hi ha més personal que la informació biomètrica? La majoria de la nostra informació personal és electiva i la podríem canviar: hem triat una religió, una ideologia política, fins i tot una orientació sexual. En canvi, les nostres dades biomètriques són les que són i no les podem canviar. Per tant, revelar-les és una pèrdua irreversible de privadesa.

De fet, la biometria és un bon exemple per mostrar que renunciar a la privadesa no necessàriament proporciona més seguretat. En primer lloc, l'ús de dades biomètriques pot ser insegur per al subjecte, si algú les roba a l'entitat que les fa servir per al control d'accés (l'entitat ha de guardar els patrons biomètrics de tots els subjectes que vol identificar, com a referència per poder-los comparar). Pitjor encara, la identificació biomètrica pot ser insegura fins i tot per a l'entitat que la fa servir: per exemple, si un atacant roba l'empremta dactilar d'un subjecte (mitjançant un atac informàtic a l'entitat o, simplement, agafant-la d'un got que hagi tocat el subjecte), amb una relativa facilitat pot fabricar un dit de silicona amb aquesta empremta i fer creure a l'entitat que és el subjecte.

El segon argument, el sacrifici de la privadesa a l'altar de la funcionalitat, és ben palès en la majoria de les aplicacions gratuïtes ofertes per les empreses d'Internet. Efectivament, els motors de cerca (Google i d'altres), les xarxes socials, els serveis de web 2.0 (Google Calendar, Street View, Latitude i d'altres), etc., es concentren a oferir funcionalitats llamineres als usuaris tot ignorant-ne completament la privadesa. Com a molt, tenen present la privadesa envers terceres parts, diferents de l'empresa que ofereix el servei o dels seus socis. En realitat, l'empresa esdevé un Gran Germà en el sentit orwel·lià.

De vegades, el segon argument ha acabat al servei del primer, com si volgués amorosir-lo. L'escàndol recent de l'Agència Nacional de Seguretat nord-americana, destapat per Edward Snowden, ha mostrat com les empreses que han aconseguit dades dels seus usuaris oferint-los funcionalitats a costa de llur privadesa poden acabar cedint-les als governs respectius en nom de la seguretat.

Els nihilistes, però, són els qui prescindeixen de tot argument i actuen sota el principi que, en un món de megadades, la privadesa és una cosa del passat. Aquest és el cas dels marxants de dades (*data brokers*). Aquests marxants recullen totes

les dades personals que troben publicades a Internet (xarxes socials, pàgines web, etc.) i aconsegueixen també dades que no són públiques però que es poden comprar (provinents de programes de fidelització, de botigues en línia, de registres de la propietat, etc.) (vegeu la figura 1). Un cop han compilat totes aquestes dades, empaqueten tota la informació corresponent a la mateixa persona, amb la qual cosa obtenen fitxes personals. Finalment, venen aquestes fitxes sense cap mena d'anonimització a qui les vulgui comprar, normalment, empreses que fan estratègies de mercat personalitzades. Segons un informe de la Comissió Federal de Telecomunicacions nord-americana (FTC, 2014), als Estats Units hi ha diversos grans marxants de dades, que operen a l'empara de la relativa permissivitat de la legislació nord-americana de protecció de dades. Per exemple, l'empresa Acxiom acumula dades personals de més de set-cents milions de persones a tot el món i té més de tres mil dades de gairebé cada consumidor nord-americà.

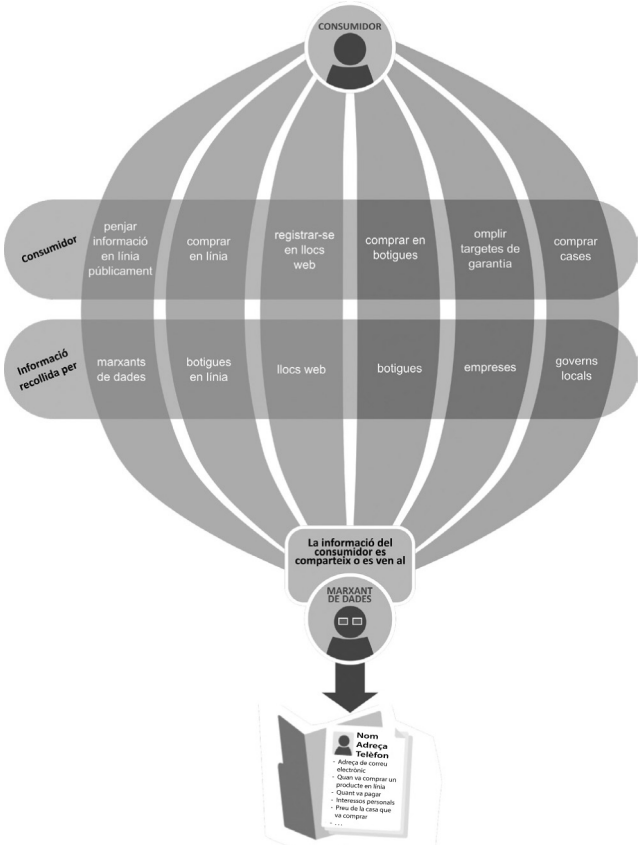

Figura 1. Captació de dades i creació de perfils per part dels marxants de dades.

Presentar Google i les grans empreses d'Internet com el Gran Germà ha fet fortuna als mitjans de comunicació i, àdhuc, a la ficció literària (vegeu Eggers, 2013, per exemple). Tanmateix, els marxants de dades són una amenaça encara més greu per a la privadesa: són el Gran Germà invisible. En primer lloc, aparellen i venen tota la informació que cada persona deixa arran de les diverses activitats de la seva vida; per tant, poden arribar a acumular molta més informació personal que una empresa d'Internet. En segon lloc, mentre que tothom sap qui són Google, Apple i Amazon, i és més o menys conscient de la informació que els forneix, la immensa majoria de la població ni tan sols sap que els marxants existeixen (i encara menys quines dades guarden). Per tant, difícilment els subjectes poden exercir llurs drets d'accés, de rectificació, d'esborrament i de petició d'oblit davant d'unes entitats que desconeixen. De fet, l'informe federal nord-americà FTC (2014) l'únic que demana als marxants és que siguin més transparents i facilitin l'exercici d'aquests drets a les persones que els ho demanin. Encara que s'hi posin bé, és improbable que els marxants rebin gaires peticions de la ciutadania, a causa del desconeixement esmentat.

La posició nihilista extrema és la dels qui proclamen públicament i sense manies que aspirar a qualsevol nivell de privadesa en la nostra societat és «delirar». És el cas de Stephen Brobst (Cuesta, 2016), el director de tecnologia de Teradata, una empresa nord-americana que es dedica des de fa més de trenta-cinc anys a l'anàlisi de dades massives. Diverses grans empreses, incloent-n'hi algunes d'implantades al nostre país, recorren regularment als serveis de Teradata per analitzar la informació que acumulen sobre clients i transaccions, amb l'objectiu de fer recomanacions i ofertes personalitzades a llurs clients. Segons Brobst, el màxim que els subjectes podem esperar és que els recol·lectors de les nostres dades no en facin un ús incorrecte.

4. Els fonamentalistes: privadesa a costa d'inutilitzar les dades

El control de la revelació estadística (CRE) és una disciplina que va iniciar-se fa quatre dècades arran del treball de Dalenius (1977) i amb l'objectiu de fer compatible la publicació de dades amb el secret estadístic. Fins a l'any 2000, les úniques organitzacions que publicaven dades de manera habitual eren els instituts d'estadística oficial dels diferents països. No ha de sorprendre, doncs, que el gros de les tècniques de CRE sorgís de la cooperació entre estadístics oficials i estadístics acadèmics. Vegeu un recull força exhaustiu d'aquestes tècniques a Hundepool *et al.* (2012).

Amb l'entrada del nou segle i l'expansió d'Internet, l'estadística oficial va perdre el monopoli *de facto* de la publicació de dades personals sensibles. Noves activitats, com la navegació per la xarxa, el comerç electrònic, els telèfons mòbils i la sensorització massiva, van començar a generar-ne grans quantitats de manera automàtica i continuada. Altres activitats preexistents, com la medicina, van infor-

matitzar-se i van donar lloc a grans fitxers de dades personals. En aquest moment, els informàtics de bases de dades van veure necessari ocupar-se de com calia publicar aquests grans fitxers que s'anaven creant sense infringir la privadesa dels subjectes (consumidors, pacients, etc.).

Val a dir que els especialistes en bases de dades van atacar el problema bastant al marge de la feina que havien fet els estadístics en el camp del CRE. És evident que aquesta manca de comunicació i de col·laboració va tenir aspectes negatius, perquè en alguns casos es va reinventar la roda, com quan en comptes de CRE es van encunyar termes com *mineria de dades amb preservació de privadesa* (*privacy-preserving data mining*, Agrawal i Srikant, 2000) i *publicació de dades amb preservació de privadesa* (*privacy-preserving data publishing*, Fung *et al.*, 2010). Ara bé, la distància també va permetre un enfocament nou: els models de privadesa esmentats anteriorment, el primer dels quals fou el *k*-anonimat (Samarati i Sweeney, 1998).

Com s'ha dit, un model de privadesa estableix una condició que les dades han de complir abans de publicar-les, de manera que, si la compleixen, pot garantir-se que la probabilitat de reidentificar un subjecte concret és baixa. En el cas del *k*-anonimat, la condició que cal complir és que, si l'atacant sap que el registre d'un cert subjecte és al fitxer publicat, com a molt, pugui determinar un conjunt de *k* registres dins del qual es troba el registre del subjecte. Per tant, si es publica un fitxer de dades *k*-anònim, la probabilitat de reidentificar el registre d'un subjecte, com a molt, és $^1/_k$. Com més gran és *k*, més privadesa hi ha. Al mateix temps, com més gran és *k*, més modificacions cal fer a un fitxer original per tal que esdevingui *k*-anònim, amb la qual cosa es perd més utilitat analítica. De tota manera, triant un *k* no gaire gran, es pot assolir un bon compromís entre privadesa i utilitat analítica (Sánchez *et al.*, 2016*b*). Vegeu un petit exemple de 2-anonimat a la taula 1.

Taula 1
Fitxer 2-anònim

Identificadors				*Quasiidentificador*					*Confidencial*
DNI	*Nom*	*Cognom 1*	*Cognom 2*	*Sexe*	*Codi postal*	*Edat*	*Data d'admissió*	*Data d'alta*	*Diagnòstic*
—	—	—	—	F	BCN	57	23/05/15	29/05/15	070.54
—	—	—	—	F	BCN	57	23/05/15	29/05/15	311.00
—	—	—	—	F	TGN	79	29/05/15	05/06/15	070.54
—	—	—	—	F	TGN	79	29/05/15	05/06/15	401.90
—	—	—	—	M	TGN	57	18/03/15	30/03/15	305.10
—	—	—	—	M	TGN	57	18/03/15	30/03/15	592.10

Nota: S'han suprimit els valors dels identificadors. El quasiidentificador és el conjunt d'atributs restants que poden servir a l'atacant per reidentificar el subjecte del registre. S'han modificat els valors del quasiidentificador, de manera que cada combinació de valors es troba repetida dos cops, amb la qual cosa s'assoleix 2-anonimat i la probabilitat que l'atacant reidentifiqui correctament el registre d'un subjecte objectiu és, com a molt, ½.

El *fonamentalisme* va arribar quan els criptògrafs van prendre el relleu dels informàtics de bases de dades en la formulació de models de privadesa. En la mentalitat del criptògraf, la prioritat absoluta és la privadesa, mentre que la utilitat analítica és secundària, si és que s'arriba a tenir en compte. És la translació del que passa amb el xifratge: a les dades xifrades no se'ls requereix que siguin útils analíticament, sinó que siguin segures.

El 2006, Dwork i altres criptògrafs van introduir el model conegut com a *privadesa diferencial* (Dwork, 2006). El model estava pensat inicialment per a consultes a bases de dades, més que no pas per a la publicació de fitxers. Es diu que un mecanisme de consulta d'una base de dades compleix la condició de privadesa diferencial si, a partir de les respostes a la consulta, és impossible determinar si un registre qualsevol és a la base de dades o no. Més precisament, donades dues bases de dades D_1 i D_2 que difereixen en un sol registre qualsevol (anomenades *bases de dades veïnes*), les probabilitats de qualsevol resultat possible de la consulta feta sobre D_1 i feta sobre D_2 difereixen en un factor no més gran que e^{ε}, on ε és un paràmetre de privadesa. La figura 2 en mostra la formulació rigorosa, en la qual f és la consulta que l'usuari vol fer i K_f és la consulta amb el soroll aleatori afegit per tal que el resultat sigui privat diferencialment. Com més petit és el paràmetre, més privadesa hi ha, de manera que $\varepsilon = 0$ vol dir que qualsevol resultat té exactament la mateixa probabilitat d'ésser obtingut sobre dues bases de dades veïnes. Per tant, la influència del registre diferent entre D_1 i D_2 sobre les respostes és nul·la, amb la qual cosa de les respostes no es pot deduir res sobre aquest registre, el subjecte del qual preserva totalment la seva privadesa.

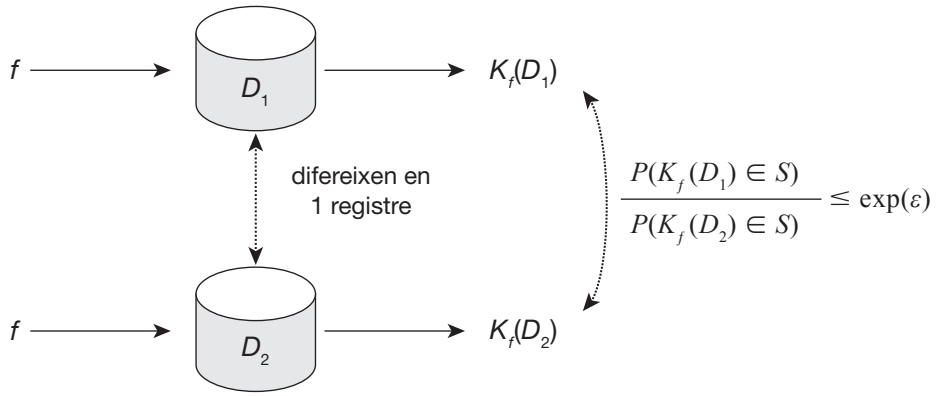

Figura 2. Privadesa diferencial.

En articles posteriors (Soria-Comas *et al.*, 2014; Xiao *et al.*, 2010; Xu *et al.*, 2012; Zhang *et al.*, 2014), hom va estendre la privadesa diferencial a la publicació

de fitxers. Bàsicament, el fitxer diferencialment privat es genera fent consultes que retornen els diferents registres amb un soroll afegit.

Ja es pot veure que si l'absència, presència o modificació de qualsevol registre no s'ha de notar en les respostes a les consultes, cal afegir molt de soroll a les respostes abans de retornar-les a l'usuari, cosa que fa que llur utilitat sigui força dubtosa. Per exemple, imaginem-nos una base de dades que contingui les rendes anuals dels habitants d'un poble petit. Si l'absència o presència del registre de l'únic milionari del poble no s'ha de notar quan es consulta la renda mitjana del poble, clarament el resultat de la consulta tindrà poc a veure amb la renda mitjana real. Encara serà pitjor si allò que es consulta és la renda màxima del poble: si no s'ha de notar l'absència o presència del milionari, vol dir que el que es retorna no té res a veure amb la renda màxima real.

No es pot negar que la definició de la *privadesa diferencial* és matemàticament elegant i que ha donat peu a una quantitat enorme de literatura acadèmica. Però sí que es pot negar que sigui pràctica. Cap institució la missió principal de la qual sigui publicar dades analíticament útils no ha fet servir la privadesa diferencial per anonimitzar-les. En els pocs exemples pràctics d'aplicació, o bé es fan servir valors de ε molt grans (per exemple, $\varepsilon = 8{,}6$ a Machanavajjhala *et al.*, 2008), que no donen cap mena de garantia de privadesa, o bé se'n preserva la utilitat només per a un estadístic molt concret (però no per a la resta). De fet, a Fredrikson *et al.* (2014) es conclou que els mecanismes actuals per assolir la privadesa diferencial no serveixen per fer recerca mèdica útil i alhora preservar la privadesa dels pacients. Per resoldre aquesta «bombolla acadèmica» originada al voltant de la privadesa diferencial, força autors busquen amb afany maneres de relaxar la condició de privadesa diferencial per fer-la menys estricta i més compatible amb la utilitat de les dades. Algunes propostes, tot i venir d'autors d'universitats de primer nivell, freguen el ridícul: és el cas de Mohan *et al.* (2012), que, després de reconèixer que la privadesa diferencial no ha estat adoptada a la pràctica, sostenen que les dades confidencials ho són menys a mesura que passa el temps, per la qual cosa es poden relaxar els paràmetres de privadesa per a dades més antigues. Una altra relaxació, publicada en una revista de primer nivell (Machanavajjhala i Kiefer, 2015), se centra a restringir la definició de *bases de dades veïnes*: ja no són bases de dades que difereixen en un registre qualsevol, sinó en algun registre d'un cert subconjunt. Encara una altra relaxació molt recent, propugnada per la creadora de la privadesa diferencial a Dwork i Rothblum (2016), s'anomena *privadesa diferencial concentrada* i és molt poc clara quant a la millora de la utilitat que ofereix.

Costa de preveure quant de temps pot trigar a esclatar la bombolla de la privadesa diferencial: és difícil continuar impulsant una cosa que ningú no vol aplicar. Certament, aquest model dóna molta privadesa, però ho fa a costa d'eliminar la utilitat de les dades. Com a molt, les dades diferencialment privades permeten de

calcular alguns estadístics molt concrets i predeterminats. En cap cas no és possible realitzar anàlisis exploratòries útils sobre dades diferencialment privades, la qual cosa fa incompatible la privadesa diferencial i les megadades (que justament serveixen per a l'anàlisi exploratòria).

5. El camí del mig en la privadesa de megadades

Se sol dir que, entre poc i massa, la mesura passa. És legítim voler aprofitar el potencial que ofereixen les megadades disponibles per millorar la vida de la humanitat en general i fins i tot per fer-hi negoci. Ara bé, cal evitar que això suposi violar la privadesa dels subjectes. Les megadades publicades haurien d'haver estat protegides, és a dir, transformades de manera que: *a*) proporcionessin resultats estadístics molt semblants als que s'obtindrien si es disposés de les megadades originals, però *b*) no permetessin de reconstruir inequívocament el perfil de cap subjecte concret.

Els mètodes de CRE (Hundepool *et al.*, 2012) (per exemple, addició de soroll, generalització, supressió, recodificació inferior i superior, microagregació i d'altres) especifiquen transformacions el propòsit de les quals és limitar el risc de revelació. Tanmateix, en general, no prescriuen cap mecanisme per avaluar quin és el risc de revelació residual de les dades transformades. En canvi, els models de privadesa —com ara el *k*-anonimat i la privadesa diferencial esmentats anteriorment, així com la *l*-diversitat (Machanavajjhala *et al.*, 2007), la *t*-proximitat (Li *et al.*, 2007) i el *k*-anonimat probabilístic (Soria-Comas i Domingo-Ferrer, 2012), entre d'altres— especifiquen algunes propietats que ha de satisfer un fitxer per limitar el risc de revelació, però no solen prescriure cap mètode de CRE concret per satisfer aquestes propietats. Els models de privadesa semblen més atractius, perquè diuen quin nivell de privadesa cal assolir i deixen llibertat al protector de les dades per adoptar el mètode menys dolent per a la utilitat analítica. La realitat, però, és que la majoria dels models de privadesa han estat concebuts per protegir un sol fitxer de dades estàtic i tenen insuficiències molt notòries a l'hora de fer-los servir en un context de megadades.

Per tal que un model de privadesa sigui útil per a megadades, ha de ser compatible amb el volum, la velocitat i la varietat d'aquesta mena de dades. Per avaluar aquesta compatibilitat, proposem de tenir en compte en quina mesura el model satisfà les tres propietats següents (Soria-Comas i Domingo-Ferrer, 2015):

— *Componibilitat*. Un model de privadesa és componible si les seves garanties de privadesa es preserven (possiblement de manera limitada) després d'aplicar-lo repetidament. Dit d'una altra manera, un model de privadesa no és componible si fitxers publicats de manera independent, cadascun dels quals satisfà el model per separat, poden portar a una violació de la privadesa quan es consideren conjunta-

ment. La componibilitat és essencial per tal que les garanties del model sobrevisquin en un context de megadades, en el qual la recollida de dades no és centralitzada, sinó distribuïda entre diverses fonts de dades. Si un dels col·lectors es preocupa de la privadesa i decideix fer servir un model de privadesa concret, les garanties de privadesa d'aquest model haurien de preservar-se (si més no, d'alguna manera) després de la fusió de les dades. La componibilitat pot avaluar-se entre fitxers publicats que satisfan el mateix model de privadesa, entre fitxers publicats que satisfan diferents models de privadesa i entre un fitxer publicat que satisfà un model de privadesa i un fitxer no anonimitzat. Aquest darrer cas és el més exigent i equival a demanar que el model de privadesa ofereixi protecció contra qualsevol coneixement previ que un atacant tingui sobre el subjecte el registre del qual vol reidentificar.

— *Cost computacional*. Aquest cost mesura la quantitat de càlcul que cal per transformar les dades originals de manera que se satisfacin els requisits del model de privadesa. Tal com hem dit anteriorment, normalment hi ha diversos mètodes de CRE que poden servir per satisfer el model de privadesa. Per tant, el cost computacional dependrà del mètode concret que es triï. És molt important que el model sigui assolible amb algun mètode eficient, atès el volum enorme de les megadades. Per anar bé, el cost del mètode hauria de ser lineal o log-lineal en la mida de les dades. Els mètodes amb costos quadràtics o superquadràtics no van bé. De tota manera, hi ha diverses modificacions que poden ajudar a fer més eficient un mètode costós d'entrada. Una d'aquestes modificacions és partir el fitxer original en diversos fitxers més petits i anonimitzar-los separadament. Evidentment, aquesta estratègia pot tenir conseqüències negatives per a la utilitat i la privadesa de les dades resultants, i caldria analitzar-les cas per cas.

— *Aparellabilitat*. En megadades, la informació d'un subjecte individual es recull de diverses fonts. Per tant, la capacitat d'aparellar registres que corresponen al mateix individu o a individus semblants és fonamental per construir megadades. Si volem preservar la privadesa dels subjectes, caldria que cada font anonimitzés les seves dades abans de publicar-les. Ara bé, si cada font anonimitza de manera independent, pot esdevenir difícil o fins i tot impossible de fusionar les dades anonimitzades de les diverses fonts. Això reduiria molt substancialment la varietat de les anàlisis que hom pot fer sobre les dades i, en conseqüència, el coneixement que hom en pot obtenir. Per ser útil en megadades, un model hauria de permetre d'alguna manera a un analista d'aparellar dades anonimitzades independentment sota aquest model que corresponen al mateix subjecte. Noteu que, quan s'aparellen registres referits al mateix subjecte, s'està incrementant la informació sobre aquest subjecte. Això és una amenaça per a la privadesa i, per tant, la precisió dels aparellaments hauria de ser més petita en fitxers anonimitzats que no pas en fitxers originals.

5.1. *Protecció de megadades amb* k*-anonimat*

Tal com s'ha esbossat més amunt, el *k*-anonimat cerca de limitar la capacitat d'un atacant per reidentificar el registre corresponent a un cert subjecte objectiu. D'una banda, el fitxer a protegir conté uns *atributs confidencials*, com ara dades mèdiques, dades econòmiques, religió, orientació sexual, etc. (si no tingués atributs confidencials, no caldria protegir-lo!). D'altra banda, conté uns atributs que anomenarem col·lectivament *quasiidentificador*; el valor de cap atribut individual del quasiidentificador en un registre no n'identifica el subjecte, però la combinació de valors de tots els atributs del quasiidentificador en el registre sí que el pot identificar. Per exemple, edat, sexe, codi postal i nivell educatiu serien un quasiidentificador, perquè en un cert codi postal pot haver-hi una sola dona de més de setanta anys que tingui el títol de doctora. De fet, el model d'atac suposa que l'atacant pot identificar almenys el subjecte d'alguns dels registres amb els atributs del quasiidentificador: una manera de fer-ho és que disposi d'una base de dades externa que contingui els atributs del quasiidentificador juntament amb identificadors (noms, DNI, etc.) per a alguns dels subjectes del fitxer a protegir. En aquest cas, aconseguirà vincular els valors dels atributs confidencials del registre del fitxer publicat amb un identificador, amb la qual cosa es produeix una revelació no desitjada. Per aconseguir reduir la probabilitat de reidentificació a $^1/_k$, el *k*-anonimat requereix que cada combinació de valors dels atributs del quasiidentificador sigui compartida per almenys *k* registres del fitxer protegit (aquest grup s'anomena *classe* k*-anònima*).

Fins i tot en l'escenari tradicional de protegir un sol fitxer estàtic, no és evident quins atributs hauria d'incloure el protector de dades en el quasiidentificador: per decidir sense equivocar-se els atributs del quasiidentificador, el protector hauria de saber exactament quin és el coneixement previ de l'atacant (i no el sap). En un escenari de megadades, el problema encara és més complicat, perquè l'atacant pot tenir molt de coneixement previ. Per anar sobre segur, val més considerar que tots els atributs, inclosos els confidencials, són part del quasiidentificador.

A banda de l'inconvenient d'haver d'establir el quasiidentificador, el *k*-anonimat té un altre problema: tot i protegir de la reidentificació, pot ser insuficient per protegir de la revelació. Aquest seria el cas quan els valors d'un atribut confidencial en els registres d'una classe *k*-anònima són iguals o molt semblants. Si l'atacant aconsegueix vincular el seu subjecte objectiu a aquesta classe, llavors, encara que no aconsegueixi saber quin dels *k* registres de la classe és el del subjecte, aconseguirà saber el valor de l'atribut confidencial per al subjecte. Això també és revelació. S'han proposat diverses extensions del *k*-anonimat per posar-hi remei, com ara la *l*-diversitat o la *t*-proximitat esmentades anteriorment.

Pel que fa a la componibilitat, el *k*-anonimat va ser dissenyat per protegir un sol fitxer i en principi no és componible. Si s'han publicat diversos fitxers *k*-anonimitzats de manera independent que comparteixen alguns subjectes, l'atacant pot valdre's de l'anomenat *atac d'intersecció* per descartar alguns dels registres de les classes *k*-anònimes com a no corresponents al seu subjecte objectiu. Per tenir una certa componibilitat, els protectors dels diversos fitxers *k*-anonimitzats s'haurien de coordinar de manera que, per als subjectes compartits entre dos fitxers, llurs classes *k*-anònimes continguin els mateixos *k* subjectes. En un entorn de megadades, això no és fàcil, però tampoc no és impossible. En cas que aquesta coordinació no sigui viable i/o que els diferents fitxers vagin creixent de manera independent al llarg del temps, a Domingo-Ferrer i Soria-Comas (2016) s'apunten diverses estratègies alternatives.

Quant al cost computacional, el *k*-anonimat se sol aconseguir modificant els valors dels atributs del quasiidentificador, sigui amb una combinació de generalitzacions i supressions (Samarati i Sweeney, 1998), sigui amb microagregació (Domingo-Ferrer i Torra, 2005). Tot i que aplicar de manera òptima aquestes modificacions (per tal de minimitzar la pèrdua d'informació) dóna lloc a problemes NP, mitjançant heurístiques i estratègies de blocatge es poden assolir complexitats $O(n \ln n)$, on n és el nombre de registres. Per tant, el *k*-anonimat és viable per a megadades.

En tercer lloc, pel que fa a l'aparellabilitat, imaginem que tenim dos fitxers *k*-anonimitzats independentment que tenen alguns subjectes en comú. Es tracta de veure si es poden aparellar els registres d'un subjecte que se sap que és a tots dos fitxers. La resposta és que, com a mínim, es poden aparellar les classes *k*-anònimes del subjecte en els dos fitxers. Si els dos fitxers comparteixen, a més, alguns atributs confidencials, la precisió de l'aparellament pot millorar, perquè podem fer servir els valors d'aquests atributs per aparellar registres concrets dins de cada classe *k*-anònima.

En resum, en un escenari de megadades, el *k*-anonimat ofereix una garantia de privadesa componible sempre que els protectors de fitxers que comparteixen subjectes es coordinin o segueixin estratègies adequades (Domingo-Ferrer i Soria-Comas, 2016). D'altra banda, hi ha heurístiques que permeten d'assolir el *k*-anonimat a un cost quasilineal en el nombre de registres. Al mateix temps, és possible d'aparellar la informació del mateix subjecte en diferents fitxers *k*-anonimitzats independentment, si més no, en l'àmbit de la classe *k*-anònima (i, en alguns casos, en l'àmbit del registre). Finalment, com més petit és el paràmetre *k*, menys cal modificar els registres originals per assolir el *k*-anonimat i més utilitat es preserva. En definitiva, amb un cert esforç de coordinació, el *k*-anonimat és una opció raonable per a l'anonimització de megadades.

5.2. *Protecció de megadades amb privadesa diferencial*

La privadesa diferencial ofereix propietats fortes de componibilitat (McSherry, 2009):

— *Composició seqüencial*. Si sobre un mateix subconjunt de subjectes es publiquen fitxers D_i, per a $i \in I$, cadascun dels quals és privat ε_i-diferencialment, el conjunt dels fitxers publicats ofereix una privadesa $\Sigma_{i \in I}\, \varepsilon_i$-diferencial. És a dir, quan s'acumulen diversos fitxers diferencialment privats sobre un conjunt de subjectes, no es trenca la privadesa diferencial, però el nivell de privadesa es redueix.

— *Composició paral·lela*. Si es publiquen diversos fitxers ε-diferencialment privats D_i, per a $i \in I$, cadascun referit a una colla de subjectes disjunta dels subjectes de la resta dels fitxers, el conjunt d'aquests fitxers és ε-diferencialment privat.

Quant al cost computacional, la privadesa diferencial s'assoleix afegint soroll a les dades originals. La quantitat de soroll necessària depèn de la sensibilitat de la consulta f que vol calcular-se, és a dir, del canvi màxim que pot sofrir f a causa de la modificació, la supressió o l'addició d'un sol registre. Si, en comptes de respondre consultes, es vol publicar un fitxer diferencialment privat, llavors f és la funció identitat. El cost d'afegir soroll és lineal en el nombre de registres, és a dir, $O(n)$.

Pel que fa a l'aparellabilitat, si tenim dos fitxers diferencialment privats en els quals s'ha afegit soroll a tots els valors de tots els atributs, en general, no serà possible d'aparellar els registres dels dos fitxers que corresponen al mateix subjecte. En canvi, si els dos fitxers comparteixen alguns atributs que s'han deixat intactes (per exemple, perquè no es consideren confidencials), aleshores poden utilitzar-se'n els valors per aparellar els registres corresponents al mateix subjecte.

Veiem, doncs, que la privadesa diferencial té propietats interessants per a les megadades: bona componibilitat, bon cost computacional i aparellabilitat, sempre que hi hagi atributs compartits i intactes entre diversos fitxers. Ara bé, tal com hem dit a l'apartat 4, el problema més gros de la privadesa diferencial és que la utilitat de les dades diferencialment privades per a anàlisis exploratòries és pràcticament inexistent per als valors de ε necessaris per assegurar una bona privadesa (típicament, per sota d'1).

Alguns autors han suggerit procediments computacionals diferents de la mera addició de soroll per mirar de millorar la utilitat de les dades diferencialment privades. Concretament, Cormode *et al.* (2012) i Zhang *et al.* (2014) proposen de sintetitzar dades diferencialment privades, amb la qual cosa poden calcular histogrames raonablement semblants als histogrames que s'haurien obtingut amb les dades originals. D'altra banda, Sánchez *et al.* (2014), Soria-Comas *et al.* (2014) i Sánchez *et al.* (2016*b*) proposen de microagregar primer els

registres del fitxer original i després aplicar soroll al fitxer microagregat per transformar-lo en un fitxer diferencialment privat. Com que els valors agregats són més estables, llur sensibilitat és més petita, amb la qual cosa cal menys soroll per atènyer la privadesa diferencial; per tant, la utilitat de les dades diferencialment privades és més gran.

Malauradament, aquests procediments més elaborats són més costosos computacionalment (Domingo-Ferrer i Soria-Comas, 2016) que la simple addició de soroll i proporcionen increments d'utilitat bastant petits, que no són suficients per a anàlisis exploratòries d'una qualitat acceptable. La raó és que, tal com s'ha dit a l'apartat 4, la mateixa definició de *privadesa diferencial* obliga a destruir la informació de cada registre per tal que no se'n noti la presència o l'absència.

6. Conclusions i línies de recerca obertes

Davant de l'eclosió de les megadades, sorgeix el debat de si són compatibles amb la privadesa dels ciutadans. D'entrada, la legislació vigent planteja uns requisits legals per a la informació identificable personalment que són molt difícils de satisfer en el cas de les megadades, tret que es disposi de bons mètodes d'anonimització. Davant d'aquest atzucac, hi ha dues posicions extremes: el nihilisme, que sosté que la privadesa és una utopia en una societat de megadades, i el fonamentalisme, que insisteix a proposar mètodes de protecció que sacrifiquen la utilitat analítica de les megadades en benefici de la privadesa. El nihilisme pot escudar-se en la seguretat o en la funcionalitat i l'eficiència. És una posició molt còmoda per a empreses, administracions i forces de seguretat, però trepitja el dret humà fonamental de privadesa (art. 12 de la Declaració Universal dels Drets Humans). En el costat oposat, el fonamentalisme és incompatible amb l'explotació de les megadades, perquè les distorsiona tant en nom de la privadesa que els lleva tota utilitat per a anàlisis exploratòries (que són el tipus d'anàlisis que se solen fer amb megadades). Per tant, el nihilisme és èticament indesitjable i el fonamentalisme és pragmàticament inviable.

Hem explorat un camí del mig entre les dues posicions extremes esmentades. Hem començat formulant algunes propietats que hauria de complir un model de privadesa per ser pràctic per a la producció de megadades prou anonimitzades i alhora prou útils analíticament: componibilitat, cost computacional baix i aparellabilitat. Tot seguit, hem examinat fins a quin punt els dos models de privadesa principals en ús, el *k*-anonimat i la privadesa diferencial, satisfan aquestes propietats. El *k*-anonimat les satisfà amb penes i treballs: per a la componibilitat, li cal que els diversos protectors de dades que generen fitxers sobre els mateixos subjectes es coordinin o segueixin unes certes estratègies; el cost computacional pot arribar a ser quasilineal si es fan servir les heurístiques adequades; l'aparellabilitat es

dóna, com a mínim, en l'àmbit de la classe *k*-anònima, però, en general, no en l'àmbit del registre. Paradoxalment, la privadesa diferencial sembla satisfer millor les tres propietats requerides: és componible i lleugera computacionalment, i ofereix aparellabilitat si alguns atributs queden sense pertorbar (no n'ofereix si es pertorben tots). Ara bé, l'argument definitiu pel qual la privadesa diferencial és pitjor que el *k*-anonimat és que, gairebé per definició, destrueix la utilitat de les dades per a anàlisis exploratòries.

Com a conseqüència del que s'ha dit, hi ha molta feina a fer per fressar aquest camí del mig. En primer lloc, caldria aconseguir un model de privadesa que fos compatible amb la componibilitat, l'eficiència de càlcul, l'aparellabilitat i la preservació de la utilitat per a anàlisis exploratòries. Això vol dir que caldria especificar no només el model, sinó també els procediments computacionals per assolir-lo. En aquest sentit, sembla que el *k*-anonimat pot ser un bon punt de partida (Domingo-Ferrer i Soria-Comas, 2016).

En segon lloc, cal reconèixer que l'accepció de *megadades* que hem fet servir a l'apartat 5 no té prou en compte llur varietat potencial: hem considerat dades estructurades de gran volum, la varietat de les quals es restringeix a la multiplicitat de fonts. Tanmateix, la varietat de les megadades pot referir-se també a llur tipus: no necessàriament han de ser dades estructurades en registres i atributs, sinó que també poden incloure vídeos, àudios, textos no estructurats, etc. La recerca de procediments d'anonimització de dades no estructurades és un camp pràcticament verge i els pocs treballs que se n'han fet es basen a censurar parts d'aquestes dades; per exemple, Sánchez i Batet (2016) presenten un model de privadesa per a la censura de documents.

En tercer lloc, no hem afrontat com es pot conciliar l'anonimització amb la velocitat de les megadades més enllà de demanar que l'anonimització sigui computacionalment eficient. Però la velocitat té més implicacions: les megadades canvien i creixen en temps real, amb la qual cosa els models de privadesa i els mètodes de CRE han de ser capaços d'anonimitzar dades canviants i creixents. Ho han de poder fer de manera eficient i alhora assegurant que un atacant no pugui violar les garanties de privadesa del model comparant les versions successives publicades dels fitxers anonimitzats. Hi ha poques contribucions a la literatura sobre l'anonimització de fluxos dinàmics de dades tradicionals (Cao *et al.*, 2011; Stokes i Torra, 2012) i pràcticament res quan es tracta de megadades dinàmiques.

Agraïments i descàrrec

La feina descrita en aquest discurs l'he feta com a catedràtic de la Universitat Rovira i Virgili, amb finançament parcial de la Generalitat de Catalunya (Premi ICREA Acadèmia i 2014 SGR 537), de la Comissió Europea (projectes H2020-

644024 «CLARUS» i H2020-700540 «CANVAS»), del Govern espanyol (projecte TIN2014-57364-C2-1-R «SmartGlacis») i de la Templeton World Charity Foundation (projecte TWCF0095/AB60 «CO-UTILITY»).

Dirigeixo la Càtedra UNESCO de Privadesa de Dades, però les opinions que he expressat són meves i no necessàriament compartides per la UNESCO.

Referències

Agrawal, R.; Srikant, R. (2000). «Privacy preserving data mining». *Proceedings of the ACM SIGMOD*, vol. 29, núm. 2 (juny), p. 439-450.

Barbaro, M.; Zeller, T. (2006). «A face is exposed for AOL searcher no. 4417749». *New York Times* (14 agost) [en línia]. <http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=0>.

Brookman, J.; Hans, G. S. (2013). «Why collection matters: surveillance as a *de facto* privacy harm». A: *Big data and privacy*: *Making ends meet* [en línia]. Palo Alto: Universitat de Stanford. Stanford Law School. The Center for Internet and Society. <https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf>.

Cao, J.; Carminati, B.; Ferrari, E. (2011). «CASTLE: continuously anonymizing data streams». *IEEE Transactions on Dependable and Secure Computing*, vol. 8, núm. 3, p. 337-352.

Chen, A. (2010). «GCreep: Google engineer stalked teens, spied on chats (updated)». *Gawker* (14 setembre) [en línia]. <http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats>.

Cormode, G.; Procopiuc, C.; Srivastava, D.; Shen, E.; Yu, T. (2012). «Differentially private spatial decompositions». A: *Proceedings of the 2012 IEEE 28th International Conference on Data Engineering - ICDE'12*. Washington: IEEE Computer Society, p. 20-31.

Cuesta, A. (2016). «*Big data* i whisky de malta». *Ara* (23 abril) [en línia]. <http://www.ara.cat/media/Big-data-whisky-malta_0_1564043647.html>.

Dalenius, T. (1977). «Towards a methodology for statistical disclosure control». *Statistisk Tidskrift*, núm. 5, p. 429-444.

Danezis, G.; Domingo-Ferrer, J.; Hansen, M.; Hoepman, J.-H.; Métayer, D. le; Tirtea, R.; Schiffner, S. (2015). *Privacy and data protection by design*: *From policy to engineering*. Informe tècnic. Khersónissos: ENISA.

Dean, J.; Ghemawat, S. (2008). «MapReduce: simplified data processing on large clusters». *Communications of the ACM*, vol. 51, núm. 1, p. 107-113.

Domingo-Ferrer, J.; Soria-Comas, J. (2016). «Anonymization in the time of big data». A: *Privacy in statistical databases - PSD 2016*. Berlín: Springer, p. 57-68.

Domingo-Ferrer, J.; Torra, V. (2005). «Ordinal, continuous and heterogeneous *k*-anonymity through microaggregation». *Data Mining & Knowledge Discovery*, vol. 11, núm. 2, p. 195-212.

Duhigg, C. (2012). «How companies learn your secrets». *New York Times Magazine* (16 febrer) [en línia]. <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.

Dwork, C. (2006). «Differential privacy». A: *33rd International Colloquium on Automata, Languages and Programming - ICALP'06*. Berlín: Springer, p. 1-12.

Dwork, C.; Rothblum, G. N. (2016). *Concentrated differential privacy* [en línia]. Ithaca: Cornell University Library. Versió 2.0, 16 març. <https://arxiv.org/pdf/1603.01887v2.pdf>.

Eggers, D. (2013). *The circle*. Londres: Penguin Books.

Fredrikson, M.; Lantz, E.; Jha, S.; Lin, S.; Page, D.; Ristenpart, T. (2014). «Privacy in pharmacogenetics: an end-to-end of personalized warfarin dosing». A: *Proceed-*

ings of the 23rd USENIX Security Symposium. San Diego: USENIX Association, p. 17-32.

FTC (2014). *Data brokers*: *A call for transparency and accountability*. Washington: US Federal Trade Commission.

Fung, B.; Wang, K.; Chen, R.; Yu, P. S. (2010). «Privacy-preserving data publishing». *ACM Computing Surveys*, vol. 42, núm. 4, p. 14.

Hansell, S. (2006). «AOL removes search data on group of web users». *New York Times* (8 agost) [en línia]. <http://www.nytimes.com/2006/08/08/business/media/08aol.html>.

Hundepool, A.; Domingo-Ferrer, J.; Franconi, L.; Giessing, S.; Schulte Nordholt, E.; Spicer, K.; Wolf, P.-P. de (2012). *Statistical disclosure control*. Chichester: Wiley.

Li, N.; Li, T.; Venkatasubramanian, S. (2007). «*t*-Closeness: privacy beyond *k*-anonymity and *l*-diversity». A: *Proceedings of the 23rd IEEE International Conference on Data Engineering - ICDE 2007*. Washington: IEEE Computer Society, p. 106-115.

Machanavajjhala, A.; Kiefer, D. (2015). «Designing statistical privacy for your data». *Communications of the ACM*, vol. 58, núm. 3, p. 58-67.

Machanavajjhala, A.; Kiefer, D.; Abowd, J.; Gehrke, J.; Vilhuber, L. (2008). «Privacy: theory meets practice on the map». A: *Proceedings of the 2008 IEEE 24th International Conference on Data Engineering - ICDE'08*. Washington: IEEE Computer Society, p. 277-286.

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

McSherry, F. D. (2009). «Privacy integrated queries: an extensible platform for privacy-preserving data analysis». A: *Proceedings of the 2009 ACM SIGMOD International Conference on Management of Data - SIGMOD'09*. Nova York: ACM, p. 19-30.

Meeker, M. (2014). «2014 Internet trends». *KPCB* (28 maig) [en línia]. <http://www.kpcb.com/blog/2014-internet-trends>.

Mohan, P.; Thakurta, A.; Shi, E.; Song, D.; Culler, D. E. (2012). «GUPT: privacy preserving data analysis made easy». A: *Proceedings of ACM SIGMOD'12*. Nova York: ACM.

Samarati, P.; Sweeney, L. (1998). *Protecting privacy when disclosing information*: k-*Anonymity and its enforcement through generalization and suppression*. Informe tècnic. Menlo Park: SRI International.

Sánchez, D.; Batet, M. (2016). «C-sanitized: a privacy model for document redaction and sanitization». *Journal of the Association for Information Science and Technology*, vol. 67, núm. 1, p. 148-163.

Sánchez, D.; Domingo-Ferrer, J.; Martínez, S. (2014). «Improving the utility of differential privacy via univariate microaggregation». A: *Privacy in statistical databases - PSD 2014*. Berlín: Springer, p. 130-142.

Sánchez, D.; Domingo-Ferrer, J.; Martínez, S.; Soria-Comas, J. (2016*a*). «Utility-preserving differentially private data releases via individual ranking microaggregation». *Information Fusion*, núm. 30, p. 1-14.

Sánchez, D.; Martínez, S.; Domingo-Ferrer, J. (2016*b*). «Comment on "Unique in the shopping mall: on the reidentifiability of credit card metadata"». *Science*, vol. 351, núm. 6279 (18 març), p. 1274.

Solove, D. J. (2011). *Nothing to hide*: *The false tradeoff between privacy and security*. New Haven: Yale University Press.

Soria-Comas, J.; Domingo-Ferrer, J. (2012). «Probabilistic *k*-anonymity through microaggregation and data swapping». A: *Proceedings of the IEEE International Conference on Fuzzy Systems - FUZZ IEEE 2012*. Washington: IEEE Computer Society, p. 1-8.

— (2015). «Big data privacy: challenges to privacy principles and models». *Data Science and Engineering*, vol. 1, núm. 1, p. 21-28.

Soria-Comas, J.; Domingo-Ferrer, J.; Sánchez, D.; Martínez, S. (2014). «Enhancing data utility in differential privacy via microaggregation-based *k*-anonymity». *VLDB Journal*, vol. 23, núm. 5, p. 771-794.

Stokes, K.; Torra, V. (2012). «Multiple releases of *k*-anonymous datasets and *k*-anonymous relational databases». *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 20, núm. 6, p. 839-853.

Xiao, Y.; Xiong, L.; Yuan, C. (2010). «Differentially private data release through multidimensional partitioning». A: *Proceedings of the 7th VLDB Conference on Secure Data Management - SDM'10*. Berlín: Springer, p. 150-168.

Xu, J.; Zhang, Z.: Xiao, X.; Yang, Y.; Yu, G. (2012). «Differentially private histogram publication». A: *Proceedings of the 2012 IEEE 28th International Conference on Data Engineering - ICDE'12*. Washington: IEEE Computer Society, p. 32-43.

Zhang, J.; Cormode, G.; Procopiuc, C. M.; Srivastava, D.; Xiao, X. (2014). «Privbayes: private data release via Bayesian networks». A: *Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data - SIGMOD'14*. Nova York: ACM, p. 1423-1434.


INSTITVT D'ESTVDIS CATALANS
MCMVII


9 788499 653242