IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monogràfic «V Congrés Internet, Dret i Política (IDP). Cara i creu de les xarxes socials»

ARTICLE

E-privadesa i xarxes socials

Antoni Roig

Data de presentació: octubre de 2009
Data d'aceptació: novembre de 2009
Data de publicación: desembre de 2009

Resum
Els riscos tecnològics per a la intimitat o privadesa no es limiten a la problemàtica de les bases de dades. Les xarxes socials, les etiquetes RFID, la computació ubiqua i la robòtica, per exemple, són altres exemples de risc per a la privadesa. Les xarxes socials tenen un valor econòmic i cada cop més enginys cerquen la informació personal dels seus usuaris. En canvi, l'estudi de la privadesa en les xarxes socials tot just és una nova àrea d'estudi. Els experts en tecnologia de la informació sovint consideren la privadesa com un atribut quantificable que es pot negociar i probablement intercanviar entre individus a canvi de certs beneficis. Nosaltres creiem, en canvi, que la regulació ha d'afavorir les anomenades *privacy enhancing technologies* (PET) o tecnologies garants de la privadesa. Aquesta garantia tecnològica de la privadesa és especialment necessària en les xarxes socials. Els drets fonamentals no poden quedar reduïts només a opcions individuals que cal activar. El component que tenen de política pública podria ser garantit si s'incorporessin versions favorables a la privadesa en el mateix disseny de les tecnologies de la informació, com per exemple la privadesa per defecte. Una altra via interessant és fer que les empreses vegin també un profit econòmic en la previsió de tecnologia garant de la privadesa.

Paraules clau
xarxes socials, tecnologies garants de la privadesa, privadesa, e-privadesa, anàlisi de xarxes socials, privadesa en el disseny

Tema
Protecció de dades

e-Privacy and Social Networks

Abstract
The technological risks for privacy and anonymity are not limited to the problems of databases. Social networks, RFID tags, ubiquitous data processing and robotics, for example, are other examples of risk. Social networks have an economic value and search engines increasingly try to access their users' personal information. In contrast, the study of privacy in social networks is a new area. Experts in information technology generally consider privacy as a quantifiable attribute which can be negotiated and probably exchanged between individuals for certain benefits. We believe, on the other hand, that regulation should favour the so-called Privacy Enhancing Technologies (PET) to guarantee privacy, and that these are particularly necessary

in social networks. Fundamental rights cannot be reduced to individual options which need to be activated. The public component of public policy could be guaranteed if versions favourable to privacy were incorporated in the design of information technologies themselves, such as privacy by default. Another way may be for businesses to see economic benefits in planning technological measures guaranteeing privacy.

Keywords
social networks, privacy-enhancing technologies, privacy, e-privacy, analysis of social networks, privacy in design

Subject
Data protection

1. La reducció de la privadesa a la protecció de dades personals en bases de dades automatitzades

A Espanya, com a la resta d'Europa, l'e-privadesa o privadesa electrònica ha quedat en bona part reduïda al dret a la protecció de dades personals en bases de dades automatitzades. Vegem-ne ràpidament el procés.[1] El punt de partida en el nostre país és l'article 18.4 de la CE, on es pot llegir: «La llei limitarà l'ús de la informàtica per tal de garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets.»

Doncs bé, en un primer moment, fins a l'any 2000, el Tribunal Constitucional no reconeix un dret autònom a la protecció de dades. La jurisprudència constitucional, basant-se en el *leading case* de l'STC 254/1993, partirà del dret a la intimitat (article 18.1 de la CE), al qual afegirà una vessant informàtica. Aquesta construcció era clarament artificial, ja que el dret a la intimitat és un dret de llibertat clàssic que només pretén preservar dels poders públics una esfera personal de llibertat. L'abstenció d'actuació de l'Estat és suficient per a garantir el dret. En canvi, el dret a la protecció de dades ha de ser garantit amb un conjunt de facultats d'actuar per part de la persona, i sovint contra l'actuació d'un altre particular i no només dels poders públics. No és fins a l'STC 292/2000 que el Tribunal Constitucional configura el dret a la protecció de dades amb més precisió, i de manera deslligada del dret a la intimitat.

Però aquesta evolució jurisprudencial, quins efectes té sobre la privadesa en general, i sobre l'e-privadesa en particular? En breu, la decisió sobre l'article 18.4 de la CE redueix els efectes de les noves tecnologies sobre els drets fonamentals a la problemàtica de les bases de dades. Per entendre-ho, cal saber que la Constitució espanyola, a diferència de la portuguesa o l'americana, per exemple, no conté cap clàusula d'actualització de drets fonamentals. Per tant, els possibles nous drets que apareguin com a conseqüència de l'extensió de les noves tecnologies de la informació i la comunicació no poden ser descoberts autònomament pel Tribunal Constitucional. L'article 18.4 de la CE és l'única referència a la informàtica en una Constitució de 1978, anterior al creixement exponencial d'Internet als noranta. Per tant, si hem acotat els problemes informàtics al dret a la protecció de dades, les altres garanties han de provenir dels drets fonamentals tradicionals: la llibertat d'expressió i d'informació, el dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge i el dret al secret de les comunicacions.

En la nostra opinió, des de l'any 2000 som en una etapa transitòria, en què s'ha resolt la precisa delimitació del dret a la protecció de dades, però on queden per resoldre altres possibles manifestacions de restriccions tecnològiques de drets fonamentals. Quan aparegui una pretensió de garantir un dret que no es pugui reconduir clarament a la intimi-

1. Per a més detalls, podeu llegir el treball: ROIG, Antoni (2002), «La protecció de les bases de dades personals. Análisi de la jurisprudencia del Tribunal Constitucional». *Revista Jurídica de Catalunya*. Núm. 2, pàg. 141-156.

tat, a la llibertat d'expressió i al secret de les comunicacions, llavors caldrà reobrir el debat sobre l'article 18.4 de la CE, o sobre la clàusula d'actualització de drets, potser a partir del dret a la dignitat humana, com proposava el magistrat Jiménez de Parga en el seu vot particular a l'STC 290/2000. Potser l'e-privadesa serà tan difícil de protegir des del dret tradicional a la intimitat com ho ha estat el dret a la protecció de dades. S'ha de tenir en compte, per exemple, que el dret a la intimitat és pensat per a possibles infraccions per part de poders públics. En canvi, la privadesa en les xarxes socials la posen en perill preferentment els particulars que ofereixen aquest servei a Internet. La possibilitat d'infracció de drets fonamentals per particulars ja ha estat reconeguda en un àmbit tan important com és el laboral, on els treballadors no renuncien als drets fonamentals quan entren a l'empresa.

La posició dominant a Europa, com s'ha dit, la té la Directiva 95/46/CE, de protecció de dades.[2] Sembla que els esforços per a obtenir un estàndard internacional sobre privadesa en les xarxes socials es basarà en principis generals de la protecció de dades personals. Tot i la importància d'aquest eventual reconeixement internacional, pensem que no s'evitaran així tots els riscos tecnològics per a la privadesa. Precisament, en les xarxes socials, no tots els riscos provenen de possibles bases de dades personals, com veurem.

2. Cap a una regulació estàndard internacional de principis basats en la protecció de dades

No és estrany que el marc regulador per a la privadesa en les xarxes socials es basi en principis generals de protecció de dades. De fet, fins i tot l'Administració Obama sembla que considera convenient el model de la Directiva europea de protecció de dades, respecte a la miscel·lània legislativa i als codis de conducta voluntaris que sovintegen als Estats Units. Així, doncs, el marc regulador el constituiran les lleis nacionals de protecció de dades que transposen la Directiva europea. Si es vol tenir un coneixement detallat i actualitzat de la interpretació de la normativa de protecció de dades, cal acudir als dictàmens i estudis jurídics de l'Agència de Protecció de Dades. A escala internacional, el Grup de l'Article 29 de la Directiva europea reuneix les principals agències de protecció de dades europees i emet informes de gran interès i novetat. Ja disposem d'un marc general d'informes que permet anticipar el contingut principal dels principis reguladors del futur estàndard internacional.

Així, en primer lloc, el Memoràndum de Roma, de 2008, és el marc principal de referència sobre xarxes socials i privadesa.[3] L'informe intenta explicar per què hi ha tan poca regulació sobre la publicació de dades personals a iniciativa dels mateixos particulars. L'explicació és doble: aquesta qüestió rellevant fora de la Xarxa, i tot just hi ha començat a ser destacada a partir de les xarxes socials; també hi ha una altra consideració sociològica, com és l'existència d'una nova generació, els anomenats *digital natives* o nadius digitals, que es caracteritza pel fet de sentir-se còmodes tot i publicar detalls, alguns cops fins i tot íntims, de la seva vida a la Xarxa. Les recomanacions del Memoràndum de Roma als legisladors són:

- Introduir l'opció d'un dret a l'ús de pseudònims.
- Assegurar-se que els proveïdors de serveis són honestos i transparents quant a la informació requerida pel servei bàsic. El consentiment dels menors també demana una solució específica.
- Obligació de notificació de qualsevol risc per a les dades personals que s'hagi produït.
- Possiblement cal atribuir més responsabilitat als proveïdors sobre les dades personals en la Xarxa.
- Introduir a l'escola la temàtica de la privadesa i de les eines protectores.

2. *Diari Oficial,* núm. L281, de 23/11/1995, pàg. 31. http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm
3. INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS (2008). «Report and Guidance on Privacy in Social Network Services (Memoràndum de Roma)». A: *43a reunió* (3-4 de març del 2008: Roma) [informe en línia]. Informe núm. 675.36.5. IWGDPT. http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

El 2008 també les agències de protecció de dades van adoptar una resolució sobre la protecció de la privadesa en els serveis de les xarxes socials.[4] De totes maneres, ens sembla més rellevant la Posició número 1 d'ENISA, de 2007 (European Network and Information Security Agency).[5] Algunes de les recomanacions que semblen més destacades són:

- Les xarxes socials han d'usar, sempre que sigui possible, una informació adaptada al context, amb l'objectiu d'educar en temps real.
- Les campanyes de conscienciació han d'anar dirigides també als programadors de programari per tal d'afavorir pràctiques i polítiques d'empresa que respectin la privadesa.
- Cal fer un estudi atent de la regulació que pugui aplicar-se a les xarxes i revisar o donar resposta adequada com a mínim a les següents qüestions:
  - Què succeeix amb el contingut d'un usuari que el proveïdor de serveis l'esborra ja que el considera correu brossa?
  - Què succeeix amb les etiquetes o comentaris a les imatges (*image-tagging*) posats per tercers?
  - Qui és responsable dels problemes de seguretat derivats de l'activitat dels usuaris?
  - Com s'han de comunicar als usuaris les polítiques de privadesa de tercers inclosos en la Xarxa?
  - Què és una dada personal en una xarxa social?
  - Quina és la posició legal del qui suplanta un perfil?
  - Algunes dades de menors, com la localització, s'han de protegir?
- S'ha d'informar els usuaris què es fa amb les seves dades abans i després de tancar el compte.
- El fenomen de les xarxes s'ha de tractar de manera controlada i transparent, sense prohibir o desaconsellar, amb campanyes als menors, als professors i als pares.

El tercer document rellevant és el Working Paper núm. 163 del Grup de Treball de l'Article 29, sobre xarxes en línia, de 12 de juny de 2009.[6] Aquest document avança en l'aplicació de la Directiva de bases de dades personals en l'àmbit de les xarxes socials.

- Els proveïdors tenen l'obligació de complir la Directiva de protecció de dades i fins i tot la Directiva d'e-privadesa si ofereixen serveis de comunicacions electròniques.
- Els proveïdors tenen l'obligació d'informar els usuaris de la seva identitat i indicar les diferents finalitats amb les quals es tracten les seves dades personals.
- Es recomana que només es puguin penjar imatges i informació de tercers amb el consentiment dels individus en qüestió.
- Els proveïdors tenen l'obligació d'advertir els usuaris del dret a la privadesa dels tercers.
- En el cas de dades sensibles el consentiment ha de ser explícit, a menys que sigui una dada pública. Si la xarxa social inclou alguna dada sensible en el perfil, ha de fer constar que és voluntari contestar. Les imatges no són dada sensible, a menys que clarament sigui usades per a revelar dades sensibles dels individus.
- Quant a les dades de tercers, fins i tot si els responsables de la xarxa informen el tercer no usuari sobre l'existència de dades personals seves, un hipotètic correu electrònic invitant-lo a ser usuari de la xarxa podria vulnerar la prohibició de l'article 13.4 de la Directiva d'e-privadesa quan es refereix a l'enviament de missatges electrònics no sol·licitats per a finalitats comercials.
- Els tercers socis de la xarxa, que ofereixen serveis addicionals i que utilitzen les dades personals de la xarxa, han d'estar advertits que han de complir també les directives esmentades.

Fins i tot hi trobem una novetat interessant, més latent en les recomanacions anteriors: l'eina preferida per a garan-

4. Adoptat a la 30a. Conferència Internacional d'Agències de Protecció de Dades i Privadesa a Estrasburg, el 17/10/2008. http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf
5. HOGBEN, G. (ed.) (octubre, 2007). «Security Issues and Recommendations for Online Social Networks». *Enisa Position Paper*. Núm. 1. http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf
6. GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (2009). *Dictamen 5/2009 sobre las redes sociales en línea* [informe en línia]. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_es.pdf

tir la privadesa és una bona seguretat i un funcionament garant de la privadesa (*privacy-friendly*) per defecte.

- Les xarxes socials han de preveure aquestes característiques favorables a la privadesa sense cost afegit i han de restringir l'accés als contactes seleccionats per l'usuari mateix. Quan l'accés al perfil d'informació va més enllà dels contactes seleccionats per l'usuari, per exemple a tots els usuaris de la xarxa social, o quan l'usuari ha d'acceptar contactes independentment de la relació que tinguin amb ell, o si la dada és indexable per un motor de cerca, ens trobem amb un accés equivalent a públic. Això pot significar que s'aplica a l'usuari la Directiva de protecció de dades, i que s'assimila així a les responsabilitats que adquireix un responsable d'una base de dades. Com que ja no és un àmbit domèstic, sinó públic, fins i tot la llibertat d'expressió ha de ser matisada amb el degut respecte al dret a la privadesa. En aquesta línia, com que no hi juga l'excepció d'ús domèstic, cal protegir els drets de tercers, sobretot en relació amb les seves dades sensibles.
- L'accés restringit als perfils no ha de ser possible amb motors de cerca interns, amb paràmetres com l'edat o l'adreça. A més, les decisions per a estendre l'accés no han de ser implícites.

Finalment destaquem la solució proposada per al cas especial dels menors: la inclusió de tecnologies garants de la privadesa o *privacy enhancing technologies*:

- Educació escolar.
- No demanar dades sensibles en el formulari de subscripció; no dirigir el màrqueting directe als menors; obtenir el previ consentiment dels pares o tutors, i separar la comunitat de menors de la d'adults.
- Desenvolupar tecnologies garants de la privadesa (PET), com per exemple avisos en forma de *pop-up* o finestres emergents en moments determinants, o programari de verificació de l'edat.
- Codi de conducta dels proveïdors.

3. Riscos no coberts per la protecció de dades: l'anàlisi de les xarxes socials

3.1. Anàlisi de xarxes socials (*social network analysis*)

L'interès econòmic que genera la informació personal continguda en les xarxes socials ha fet que no només creixin projectes comercials a partir de la direcció de la xarxa, amb socis tercers, sinó que apareixen cada cop més eines d'anàlisi de xarxes per particulars no lligats a la xarxa. Inicialment eren eines matemàtiques senzilles lligades a la teoria de grafs, i a tècniques bàsiques sociològiques. Avui, s'han tornat cada cop més complexes, i inclouen interacció social i sistemes de reputació. Els usuaris ja no són només els sociòlegs o els estudiosos de les comunitats en línia, sinó fins i tot particulars o professionals que busquen col·laboradors. Eines com VisoLink se centren, doncs, en l'usuari i plantegen reptes per a la privadesa.[7] Les xarxes ja no serveixen només per a l'esbarjo, sinó que cada cop més professionals col·laboren en xarxes. En el terreny de la ciència mèdica, per exemple, és vital poder intercanviar informació sobre casos clínics i metodologies en el temps més curt possible, així com crear bases de dades històriques.[8]

Però el risc no prové només de motors de cerca externs d'abast cada cop més universal i fins i tot personalitzat. El perill per a la privadesa està també en la captura d'informació personal que l'usuari involuntàriament ha posat a la xarxa. Aquí no hi ha cap base de dades, ni tan sols una font estructurada o una dada personal explícita. Malgrat tot, una investigació duta a terme en una xarxa social concreta ha revelat que el nom del 72% dels usuaris i el nom complet del 30% dels usuaris podia deduir-se fàcilment dels perfils amb tècniques estadístiques i heurístiques. Així mateix, l'edat del 15% dels usuaris i almenys

7. FAN, L.; LI, B. (2008). «VisoLink: A User-Centric Social Relationship Mining». A: G. WANG [*et al.*] (eds.). *RSKT 2008*, *Lecture Notes in Artificial Intelligence*. Núm. 5009, pàg. 668-675.
8. VERAGO, R; CEDRATI, F. C.; D'ALESSI, F; ZANETTE, A. (2008). «Eye Knowledge Network: A Social Network for the Eye Care Community». A: M. D. Lytras [*et al.*] (eds.). *WSKS 2008*, *Lecture Notes in Artificial Intelligence*. Núm. 5288, pàg. 22-30.

una escola del 42% dels usuaris podia també deduir-se de les dades penjades en la xarxa social.[9]

3.2. El Web 3.0, amb els serveis del Web semàntic, augmenta aquest risc per a la privadesa

De fet, amb la creixent implantació de la tecnologia del Web semàntic, on els motors de cerca ja no es limitaran a les paraules clau, sinó als significats, aquests riscos per a la privadesa encara seran més importants. De fet, les aplicacions de web semàntic afegiran a l'anàlisi de les xarxes socials la possibilitat d'extreure ontologies, és a dir mapes de significat, de les pàgines web. D'aquesta manera, s'obtindrà no només l'ontologia de coneixement tècnic elaborada per un expert, sinó una nova estructura de significat basada en les relacions en la comunitat en xarxa, una semàntica emergent.[10] La mateixa noció de dada personal queda aquí mortalment afeblida, ja que la tecnologia permet extreure dades personals, cada cop amb més precisió i complexitat, de contextos desestructurats i sense aparentment capacitat d'identificar ningú. La inclusió de la IP en el grup de les dades personals va sorprendre en el seu moment. Ara ens enfrontem al risc que la capacitat de transformar en personals (identificables) un conjunt de dades aparentment innòcues estigui arribant a nivells encara més inversemblants.

4. Les *privacy enhancing technologies* (PET) o tecnologies garants de la privadesa

Un jurista sol considerar la tecnologia com un risc per a la privadesa. Això pot ser efectivament així, com s'ha dit abans. Ara bé, estem arribant a un nivell de possibilitats tècniques tan alt que fa difícil fins i tot defensar alguns drets com la privadesa sense recórrer a contramesures tècniques. Aquesta és la idea de les PET o tècniques garants: no només la tecnologia aquí no és el risc, sinó que pot ser fins i tot, si es donen unes circumstàncies, una manera de protegir efectivament el dret. Els principis o recomanacions als legisladors tímidament apunten aquesta possibilitat. Els enginyers, a força de subvencions públiques en projectes de recerca europeus, ja han començat a proposar prototipus que aviat seran adoptats per les xarxes socials.[11] Vegem algunes de les possibilitats i capacitats d'aquests enginys protectors.

4.1. La protecció tecnològica contra els motors de cerca o mineria de dades: el *privacy-preserving data mining* (P2DM)

La protecció tecnològica de la privadesa és una àrea nova, amb menys de 10 anys, i amb un plantejament encara molt teòric. En canvi, el *privacy-preserving data mining* (P2DM) és l'excepció. L'objectiu del P2DM és evitar tant com es pugui fer pública informació personal dels usuaris de la xarxa quan s'analitzin les seves dades amb finalitats estadístiques. Una eina de protecció de la privadesa en les xarxes ha de tenir en compte no només els atributs dels usuaris, sinó també les seves relacions.[12]

4.2. La protecció tecnològica de l'accés, de la identificació i dels sistemes de reputació

Les xarxes es basen en la confiança. Normalment la confiança s'obté amb el coneixement de l'altre. Això fa que es consideri habitualment que com més confiança més dades personals identificables (PII, en anglès) de l'altre es vol tenir, i per tant més risc per a la privadesa.

Per a trencar aquesta lògica perversa, s'ha pensat en primer lloc en mecanismes d'autentificació o de reconeixement, sense identificació. La idea és tenir alhora privadesa i confiança. Una forma de fer-ho és mitjançant

9. LAM, I.-F.; CHEN, K.-T.; CHEN, L.-J. (2008). «Involuntary Information Leakage in Social Network Services». A: K. MATSUURA; E. FUJISAKI (eds.) (2008). *IWSEC*, *Lecture notes in Computer Science*. Núm. 5312, pàg. 167-183.
10. MIKA, P. (2007). *Social Networks and the Semantic Web*. Nova York: Springer.
11. Workshop on Privacy and Protection in Web-based Social Networks, 8 de juny de 2009, en el marc de la International Conference on Artificial Intelligence and Law, Barcelona, en prensa.
12. WANG, D.-W.; LIAU, C.-L.; HSU, T.-S. (2006). «A GrC-Based Approach to Social Network Data Protection». A: S. GRECO [*et al.*] (eds.) (2006). *RSCTC*, *Lecture Notes in Artificial Intelligence*. Núm. 4259, pàg. 438-447.

l'ús de pseudònims, que és una de les recomanacions als legisladors més habituals de les agències de protecció de dades i grups d'experts. Ara bé, aquesta solució tampoc és definitiva: l'anàlisi de la xarxa social i la mineria de dades poden aconseguir associar estadísticament un pseudònim a un usuari real. Per això, els experts recomanen l'ús de múltiples pseudònims. Existeixen solucions tècniques per a evitar el mal ús dels múltiples pseudònims.[13] En la mateixa línia, el projecte europeu PRIME (Privacy and Identity Management for Europe) fa ús de credencials privades. Aquestes credencials serveixen de prova de les autoritzacions, per exemple de ser major d'edat, sense identificar l'usuari. Només en cas de mal ús l'anonimat pot ser revocat.[14]

Com hem dit, les xarxes adopten sistemes de reputació per a garantir la confiança. Ara bé, els actuals sistemes de reputació generen perfils de l'usuari que inclouen tots els contextos en els quals aquest ha intervingut. Això sovinteja en les xarxes de compravenda electrònica, en les quals el temps, la freqüència de la participació, l'avaluació i l'interès per certs productes pot ser controlat. A més, els actors econòmics solen tenir el seu pseudònim vinculat a un nom real, cosa que fa que el perfil sigui plenament identificat. Un altre risc en els sistemes de reputació es deu als diferents tipus de relacions entre usuaris, com per exemple «amic de». El 2006, milers d'usuaris de Facebook van protestar per una utilitat anomenada News Feed, que informava de la darrera informació personal dels usuaris catalogats com a amics.[15] Per a aturar l'allau de crítiques, Facebook va permetre als usuaris disposar d'algunes preferències de privadesa. Més endavant, el novembre de 2007, un altre servei de Facebook va generar controvèrsia: Beacon.[16] Beacon forma part del sistema d'alertes de Facebook, que segueix les activitats dels usuaris en la navegació pels llocs web dels seus *partners*. Aquesta navegació era posada a disposició dels amics de l'usuari, sense el seu consentiment. De nou les xarxes socials han reaccionat davant les crítiques, i han ofert als usuaris mecanismes opcionals que permeten o no l'accés a la seva informació personal (www.facebook.com, http://videntity.org).

Ara bé, són necessàries estratègies més flexibles, que permetin a l'usuari definir la seva política privada personal. La idea és que els usuaris indiquin quins usuaris estan autoritzats a accedir a la seva pàgina personal, fins i tot si no són usuaris connectats amb una relació d'amistat.[17] Una opció és a través d'un control d'accés per part de l'usuari mateix,[18] o a través de la col·laboració d'un grup d'usuaris seleccionats o sense un nòdul central.[19] Dit això, el control d'accés no és l'única manera de preservar la privadesa a les xarxes socials. És necessari plantejar altres sistemes de reputació garants de la privadesa des d'una òptica més general.

4.3. Sistemes de reputació garants de la privadesa, no basats en l'accés

Ja hem indicat que les recomanacions de les agències de protecció de dades en el sentit d'usar pseudònims s'haurien de traduir en una multiplicitat de pseudònims. Ja hem dit que cal evitar-ne el mal ús. Ara ens interessa afe-

13. SEIGNEUR, J. M. (2009). «Social Trust of Virtual Identities». A: J. Golbeck (ed.). *Computing with Social Trust*. Londres: Springer-Verlag. Human-Computer Interaction Series.
14. HANSEN, M. (2008). «Marrying Transparency Tools with User-Controlled Identity Management». A: S. FISCHER-HÜBNER; P. DUQUENOY; A. ZUCCATO; L. MARTUCCI. *The Future of Identity in the Information Society*. IFIP International Federation for Information Processing. Vol. 262, pàg. 199-200. Boston: Springer.
15. CHEN, L. (2006, octubre). «Facebook's feeds cause privacy concerns. The amherst student». http://halogen.note.amherst.edu/ astudent/2006-2007/issue02/news/01.html
16. BERTEAU, S. (2007). «Facebook's misrepresentation of beacon threats to privacy: Tracking users who opt out or are not logged in». http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-trackingusers-who-opt-out-or-are-not-logged-in.aspx
17. CARMINATI B.; FERRARI, E. (2008). «Privacy-Aware Collaborative Access Control in Web-Based Social Networks». A: V. ATLURI (ed.). *DAS, Lecture Notes in Computer Science*. Núm. 5094, pàg. 81-96.
18. CARMINATI B.; FERRARI, E.; PEREGO, A. (2007). «Private relationships in social networks». A: *ICDE 2007 Workshops Proceedings*. Los Alamitos: IEEE CS Press. Pàg. 163-171.
19. DOMINGO-FERRER, J. (2007). «A Public-Key Protocol for Social Networks with Private Relationships». A: V. TORRA; Y. NARUKAWA; Y. YOSHIDA (eds.). *MDAI 2007, Lecture Notes in Artificial Intelligence*. Núm. 4617, pág. 373-379.

gir que es pot obtenir un sistema de reputació fiable amb valoracions dels pseudònims en diferents contextos. Aquest esquema ha estat fins i tot proposat per a xarxes de P2P amb pseudònims.[20] Es disposa d'uns punts de reputació (*e-cash*). Un usuari honest pot canviar el seu pseudònim i conservar la seva reputació. En canvi, un usuari deshonest no pot esborrar el seu compte de punts ni tant sols canviant de pseudònim.

4.4. Tecnologia per a la transparència, el context i la finalitat

Les tecnologies garants de la privadesa tradicionals han buscat l'anonimització, la pseudoanonimització i l'autenticació. Sembla que hi ha una tendència que afavoreix actualment les PET més centrades en la transparència. En tot cas són estratègies complementàries. Segurament la implantació progressiva de la normativa europea sobre protecció de dades, molt centrada en el control de la informació i en la finalitat, pot explicar, si més no parcialment, aquest nou enfocament.

Les tecnologies de la transparència han de garantir que el flux d'informació sigui visible i deixi traça. I això es pretén de manera àmplia, de manera que afecti les polítiques de privadesa, el processament de les dades, els serveis oferts, el programari utilitzat, els *partners*, la confiança, així com possibles problemes de seguretat. Les eines de transparència totes soles no solucionen els riscos per a la privadesa. Només la combinació d'aquestes eines amb la gestió de la identitat i els sistemes de reputació pot oferir garanties per a la privadesa.

Una possibilitat extrema és la de les TET (*transparency enhancing technologies*), que pretén anticipar un possible perfil que es pugui deduir de les dades d'un particular. La idea central és disposar de prou informació per a ser capaç de construir un perfil contrari al que es dedueix de la informació disponible. L'ús més habitual de la tecnologia de la transparència, però, és poder saber a cada moment quina dada personal s'ha donat al sistema, per tal d'accedir-hi, alterar-la o esborrar-la. En el projecte europeu PRIME, el «cercador de dades» o «*data track*» compleix aquesta funció. Abans de donar informació personal es pot consultar l'activitat dels *partners* i la política de privadesa. Aquesta informació serveix també per a demanar als responsables de les dades si han actuat correctament o per a investigar riscos detectats en anteriors utilitzacions del cercador de dades.

Conclusions

La protecció de la privadesa en les xarxes socials no és l'adequada. Diverses raons coincideixen en aquesta situació delicada:

- El marc regulador és inexistent o molt limitat. Només la regulació sobre la protecció de les bases de dades personals configura un cos destacat. Ara bé, la vigència plena d'aquest marc se centra en els països europeus. Hi ha, però, una tasca molt notable de les agències de protecció de dades i dels grups de treball propers a aquestes agències que concreta mesures i recomanacions útils. En aquest sentit, ara es mira d'arribar a un estàndard internacional de privadesa en les xarxes socials que pot resultar un primer marc regulador de referència en la matèria. Ara bé, la reducció de tota la problemàtica a la protecció de les bases de dades exclou aspectes rellevants de la protecció de la privadesa en les xarxes socials que cal no oblidar.
- La tecnologia de protecció de la privadesa per primera vegada apareix tímidament en algunes recomanacions. La debilitat és doble. D'un costat, no hi ha una fonamentació jurídica de la tecnologia com a garant de drets. Més aviat al contrari, la tecnologia és vista com a font de riscos per als drets. Una possible fonamentació pot venir del principi de proporcionalitat, que regeix les limitacions de drets. Simplificant, la necessitat d'una restricció de drets es valora per la impossibilitat de dur a terme una finalitat legítima, com pot ser la gestió d'una xarxa social, amb una afectació més petita als drets. Doncs bé, si les PET o tecnologies garants de la privadesa fossin d'abast públic, es podrien qüestionar les restriccions de la privadesa com a mesures desproporcionades, per innecessàries. De l'altre costat, les PET tenen moltes dificultats de passar del nivell teòric dels projectes europeus, que és on apareixen, al poste-

20. ANDROULAKI, E.; CHOI, S. G.; BELLOVIN, S. M.; MALKIN, T. «Reputation Systems for Anonymous Networks». A: N. BORISOV; I. GOLDBERG (eds.). *PETS 2008, Lecture Notes in Computer Science*. Núm. 5134, pàg. 202-218.

rior desenvolupament i aplicació comercial. No sembla que hi hagi impuls públic, ni consciència particular de la situació delicada, i per ara són vistes per la indústria com una despesa extra no imposada per cap llei, ni sancionada per cap agència.

- Les xarxes socials són un terreny especialment vulnerable per a la privadesa. Però no són l'únic: la computació ubiqua, les etiquetes RFID i la robòtica, segons els nostres limitats coneixements, són igualment reptes molt difícils. Una possible aproximació, més anglosaxona, consisteix a fer que la indústria tingui interès econòmic a desenvolupar eines que incorporin una versió «amiga de la privadesa». L'interès d'aquesta proposta consisteix en el fet que les solucions són més senzilles i més barates si ja s'incorporen en el disseny del sistema o programa que si s'hi intenta afegir *a posteriori* un «paquet» addicional de PET. Potser per això les mateixes PET van incorporant altres opcions a més de les tradicionals basades en l'anonimat, els pseudònims i les autenticacions. Sembla, però que s'hi dibuixa un risc: la negociació de les facultats o drets entre l'usuari i la xarxa social, o entre usuaris, a canvi de beneficis transforma els drets fonamentals en opcions individuals. Potser la privadesa pot acabar de diluir-se en aquest mercat d'intercanvis o de concessions. Per això, volem destacar un dictamen, en el marc de les etiquetes RFID, del Supervisor Europeu de Protecció de Dades, que per desgràcia encara no sembla que hagi arribat a les propostes de les agències sobre xarxes socials: la previsió de les mesures tecnològiques garants de la privadesa en el mateix moment del disseny de l'eina.[21] Aquest repte no és només per als enginyers de les PET, que hauran de pensar «en temps real» i en el context específic d'un producte comercial; també ho és per al dret, si no ens volem quedar, en el millor dels casos, amb una llista de principis generals. La previsió d'estàndards tècnics protectors de la privadesa pot ser la darrera oportunitat per a la regulació, entesa com a competició entre els interessos comercials particulars i els interessos generals com la privadesa. La redefinició de la privadesa es farà, presumiblement, no en grans definicions, sinó en petites i constants redefinicions de tècniques garants en àmbits com les xarxes socials. Si no estem atents, el dret a la privadesa pot acabar essent només un «dret ficció».

Referències

ANDROULAKI, E.; CHOI, S. G.; BELLOVIN, S. M.; MALKIN, T. «Reputation Systems for Anonymous Networks». A: N. BORISOV; I. GOLDBERG (eds.). *PETS 2008, Lecture Notes in Computer Science*. Núm. 5134, pàg. 202-218.

BERTEAU, S. (2007). «Facebook's misrepresentation of beacon threats to privacy: Tracking users who opt out or are not logged in».

‹http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-trackingusers-who-opt-out-or-are-not-logged-in.aspx›

CARMINATI B.; FERRARI, E. (2008). «Privacy-Aware Collaborative Access Control in Web-Based Social Networks». A: V. ATLURI (ed.). *DAS*, *Lecture Notes in Computer Science*. Núm. 5094, pàg. 81-96.

CARMINATI B.; FERRARI, E.; PEREGO, A. (2007). «Private relationships in social networks». A: *ICDE 2007 Workshops Proceedings*. Los Alamitos: IEEE CS Press. Pàg. 163-171.

CHEN, L. (2006, octubre). «Facebook's feeds cause privacy concerns. The amherst student». ‹http://halogen.note.amherst.edu/ astudent/2006-2007/issue02/news/01.html›

21. Dictamen del Supervisor Europeu de Protecció de Dades relatiu a la Comunicació de la Comissió al Parlament Europeu, al Consell, al Comitè Econòmic i Social Europeu i al Comitè de les Regions «La identificació per radiofreqüència (RFID) a Europa: Passes cap a un marc polític», document COM (2007) 96, (2008/C101/01), on parla de la necessitat «d'intimitat mitjançant el disseny».

DOMINGO-FERRER, J. (2007). «A Public-Key Protocol for Social Networks with Private Relationships». A: V. TORRA; Y. NARUKAWA; Y. YOSHIDA (eds.). *MDAI 2007*, *Lecture Notes in Artificial Intelligence*. Núm. 4617, pág. 373-379.

FAN, L.; LI, B. (2008). «VisoLink: A User-Centric Social Relationship Mining». A: G. WANG [*et al.*] (eds.). *RSKT 2008*, *Lecture Notes in Artificial Intelligence*. Núm. 5009, pàg. 668-675.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (2009). *Dictamen 5/2009 sobre las redes sociales en línea*
[informe en línia].
‹http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_es.pdf›

HANSEN, M. (2008). «Marrying Transparency Tools with User-Controlled Identity Management». A: S. Fischer-Hübner; P. Duquenoy; A. Zuccato; L. Martucci. *The Future of Identity in the Information Society*. IFIP International Federation for Information Processing. Vol. 262, pàg. 199-200. Boston: Springer

HOGBEN, G. (ed.) (octubre, 2007). «Security Issues and Recommendations for Online Social Networks». *Enisa Position Paper*. Núm. 1.
‹http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf›

INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS (2008). «Report and Guidance on Privacy in Social Network Services (Memoràndum de Roma)». A: *43a reunió* (3-4 de març del 2008: Roma) [informe en línia]. Informe núm. 675.36.5. IWGDPT.
‹http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491›

LAM, I.-F.; CHEN, K.-T.; CHEN, L.-J. (2008). «Involuntary Information Leakage in Social Network Services». A: K. MATSUURA; E. FUJISAKI (eds.) (2008). *IWSEC*, *Lecture notes in Computer Science*. Núm. 5312, pàg. 167-183.

MIKA, P. (2007). *Social Networks and the Semantic Web*. Nova York: Springer.

SEIGNEUR, J. M. (2009). «Social Trust of Virtual Identities». A: J. Golbeck (ed.). *Computing with Social Trust*. Londres: Springer-Verlag. Human-Computer Interaction Series.

VERAGO, R; CEDRATI, F. C.; D'ALESSI, F; ZANETTE, A. (2008). «Eye Knowledge Network: A Social Network for the Eye Care Community». A: M. D. Lytras [*et al.*] (eds.). *WSKS 2008*, *Lecture Notes in Artificial Intelligence*. Núm. 5288, pàg. 22-30.

WANG, D.-W.; LIAU, C.-L.; HSU, T.-S. (2006). «A GrC-Based Approach to Social Network Data Protection». A: S. GRECO [*et al.*] (eds.) (2006). *RSCTC*, *Lecture Notes in Artificial Intelligence*. Núm. 4259, pàg. 438-447.

Citació recomanada

ROIG, Antoni (2009). «E-privadesa i xarxes socials». A: «V Congrés Internet, Dret i Política (IDP). Cara i creu de les xarxes socials» [monogràfic en línia]. *IDP. Revista d'Internet, Dret i Política*. Núm. 9. UOC. [Data de consulta: dd/mm/aa].

‹ http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_roig/n9_roig_cat›

ISSN 1699-8154

Sobre l'autor

Antoni Roig
antoni.roig@uab.cat

El Dr. Antoni Roig és professor de Dret constitucional a la Facultat de Dret de la UAB. Ha estat investigador en projectes nacionals i europeus. Ha publicat en les àrees de fonts del dret, dret europeu, bases de dades, tecnologia i llibertat d'expressió i privacitat de ciutadans i treballadors. Les últimes publicacions s'han centrat en la privacitat i el govern electrònic.

Doctorat en Dret per la UAB, ha fet estudis postdoctorals a les Universidad Cattolica di Milano (Milà, 1996-1997) i Università degli Studi di Firenze (Florència, 1997). En l'actualitat, participa en un curs d'enginyeria tècnica informàtica a la Universitat Oberta de Catalunya.

IDT, Institut de Dret i Tecnologia
Universitat Autònoma de Barcelona
08193 Bellaterra (Barcelona), Espanya