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

http://idp.uoc.edu

Monográfico «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales»

ARTÍCULO

E-privacidad y redes sociales

Antoni Roig

Fecha de presentación: octubre de 2009
Fecha de aceptación: noviembre de 2009
Fecha de publicación: diciembre de 2009

Resumen

Los riesgos tecnológicos para la intimidad o la privacidad no se limitan a la problemática de las bases de datos. Las redes sociales, las etiquetas RFID, la computación ubicua y la robótica, por ejemplo, son otros ejemplos de riesgo para la privacidad. Las redes sociales también poseen valor económico y por ello cada vez se crean más ingenios que buscan la información personal de sus usuarios. En cambio, el estudio de la privacidad en las redes sociales es sólo una nueva área de estudio. A menudo, los expertos en tecnología de la información consideran la privacidad como un atributo cuantificable que se puede negociar y, probablemente, intercambiar entre individuos a cambio de ciertos beneficios. Nosotros creemos, en cambio, que la regulación debe favorecer las denominadas privacy enhancing technologies (PET) o tecnologías garantes de la privacidad. Esta garantía tecnológica de la privacidad es especialmente necesaria en las redes sociales. Los derechos fundamentales no pueden quedar reducidos sólo a opciones individuales que es preciso activar. Su componente de política pública podría estar garantizado si se incorporaran versiones favorables a la privacidad en el mismo diseño de las tecnologías de la información, como la privacidad por defecto. Otra vía interesante es conseguir que las empresas encuentren también un provecho económico en la previsión de tecnología garante de la privacidad

Palabras clave

redes sociales, *privacy-enhancing technologies*, privacidad, e-privacidad, análisis de redes sociales, privacidad en el diseño

Tema

Protección de datos

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 reducción de la privacidad en la protección de datos personales en bases de datos automatizadas

En España, como en el resto de Europa, la e-privacidad o privacidad electrónica ha quedado, en buena medida, reducida al derecho a la protección de datos personales en bases de datos automatizadas. Veamos rápidamente el proceso.[1] El punto de partida en nuestro país es el artículo 18.4 CE, en el que se puede leer: «La ley limitará el uso de la informática con el fin de garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

Pues bien, en un primer momento, hasta el año 2000, el Tribunal Constitucional no reconocerá un derecho autónomo a la protección de datos. La jurisprudencia constitucional, basándose en el *leading case* de la STC 254/1993, partirá del derecho a la intimidad (artículo 18.1 CE), al que añadirá una vertiente informática. Esta construcción era claramente artificial, ya que el derecho a la intimidad es un derecho de libertad clásico que sólo pretende preservar de los poderes públicos una esfera personal de libertad. La abstención de actuación del Estado es suficiente para garantizar el derecho. En cambio, el derecho a la protección de datos debe ser garantizado junto a una serie de facultades de actuación por parte de la persona y, a menudo, contra la actuación de otro particular, y no sólo de los poderes públicos. Hasta la STC 292/2000 el Tribunal Constitucional no configurará el derecho a la protección de datos con más precisión, y de manera separada del derecho a la intimidad.

Pero ¿qué efectos tiene esta evolución jurisprudencial sobre la privacidad, en general, y sobre la e-privacidad, en particular? Resumidamente, la decisión sobre el artículo 18.4 CE ha reducido los efectos de las nuevas tecnologías sobre los derechos fundamentales en la problemática de las bases de datos. Para entenderlo, es preciso saber que la Constitución española, a diferencia de la portuguesa o la americana, por ejemplo, no contiene ninguna cláusula de actualización de derechos fundamentales. Por lo tanto, los posibles nuevos derechos que aparezcan como consecuencia de la extensión de las nuevas tecnologías de la información y la comunicación no pueden ser descubiertos autónomamente por el Tribunal Constitucional. El artículo 18.4 CE es la única referencia a la informática en la Constitución de 1978, anterior al crecimiento exponencial de Internet en los años noventa. Por lo tanto, si hemos acotado los problemas informáticos al derecho a la protección de datos, las otras garantías deberán provenir de los derechos fundamentales tradicionales: la libertad de expresión y de información, el derecho al honor, a la intimidad personal y familiar y a la propia imagen, y el derecho al secreto de las comunicaciones.

1. Para más detalles, podéis leer el trabajo: ROIG, Antoni (2002). «La protecció de les bases de dades personals. Análisi de la jurisprudencia del Tribunal Constitucional». *Revista Jurídica de Catalunya*, n.º 2, pág. 141-156.

En nuestra opinión, desde el año 2000 estamos en una etapa transitoria, en la que se ha resuelto la precisa delimitación del derecho a la protección de datos, pero en la que quedan por resolver otras posibles manifestaciones de restricciones tecnológicas de derechos fundamentales. Cuando aparezca una pretensión de garantizar un derecho que no se pueda reconducir claramente a la intimidad, a la libertad de expresión y al secreto de las comunicaciones, será necesario reabrir el debate sobre el artículo 18.4 CE, o sobre la cláusula de actualización de derechos, quizá a partir del derecho a la dignidad humana, como proponía el magistrado Jiménez de Parga en su voto particular en la STC 290/2000. La e-privacidad quizá será tan difícil de proteger desde el derecho tradicional a la intimidad como lo ha sido el derecho a la protección de datos. Téngase en cuenta, por ejemplo, que el derecho a la intimidad está pensado para posibles infracciones por parte de poderes públicos. En cambio, la privacidad en las redes sociales la ponen en peligro, preferentemente los particulares que ofrecen este servicio en Internet. La posibilidad de infracción de derechos fundamentales por particulares ya ha sido reconocida en un ámbito tan importante como el laboral, en el que los trabajadores no renuncian a sus derechos fundamentales cuando entran en la empresa.

La posición dominante en Europa, como se ha indicado, la tiene la Directiva 95/46/CE, de Protección de Datos.[2] Parece que los esfuerzos por obtener un estándar internacional sobre privacidad en las redes sociales se basarán en principios generales de la protección de datos personales. A pesar de la importancia de este eventual reconocimiento internacional, pensamos que no se evitarán así todos los riesgos tecnológicos para la privacidad. Precisamente, en las redes sociales no todos los riesgos provienen de posibles bases de datos personales, como veremos.

2. Hacia una regulación estándar internacional de principios basados en la protección de datos

No es extraño que el marco regulador para la privacidad en las redes sociales se base en principios generales de protección de datos. De hecho, incluso la Administración Obama parece considerar conveniente el modelo de la Directiva europea de Protección de Datos, frente a la miscelánea legislativa y a los códigos de conducta voluntarios que menudean en Estados Unidos. Así pues, el marco regulador lo constituirán las leyes nacionales de protección de datos que incorpora la Directiva europea. Si se desea tener un conocimiento detallado y actualizado de la interpretación de la normativa de protección de datos, es necesario acudir a los dictámenes y estudios jurídicos de la Agencia de protección de datos. En un ámbito internacional, el grupo del artículo 29 de la Directiva europea reúne a las principales agencias de protección de datos europeos y emite informes de gran interés y novedad. Ya disponemos de un marco general de informes que permite anticipar el contenido principal de los principios reguladores del futuro estándar internacional.

Así, en primer lugar, el Memorándum de Roma del 2008 es el marco principal de referencia sobre redes sociales y privacidad.[3] El informe intenta explicar por qué hay tan poca regulación sobre la publicación de datos personales a iniciativa de los propios particulares. La explicación sería doble: no ha sido ésta una cuestión relevante fuera de la Red, y sólo ha empezado a destacar en ésta a partir de la aparición de las redes sociales; otra consideración sería sociológica, en este caso la existencia de una nueva generación, los denominados «digital natives» o nativos digitales, que se caracterizarían por sentirse cómodos a pesar de publicar detalles, algunas veces incluso íntimos, de su vida

2. *Diario Oficial*, n.º L281 de 23/11/1995, pág. 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 (Memorandum de Roma)». En: *43.ª reunión* (3-4 de marzo del 2008: Roma) [informe en línea]. Informe n.º 675.36.5. IWGDPT.
http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

en la Red. Las recomendaciones del Memorándum de Roma a los legisladores serían:

- Introducir la opción de un derecho al uso de seudónimos.
- Asegurarse de que los proveedores de servicios sean honestos y transparentes en cuanto a la información requerida por el servicio básico. El consentimiento de los menores también demandará una solución específica.
- Obligación de notificación de cualquier riesgo para los datos personales que se haya podido producir.
- Posiblemente será necesario atribuir más responsabilidad a los proveedores sobre los datos personales en la Red.
- Introducir en la escuela la temática de la privacidad y de las herramientas protectoras.

En el año 2008 también se adoptó una resolución sobre la protección de la privacidad en los servicios de las redes sociales por parte de las agencias de protección de datos.[4] De todas maneras, nos parece más relevante la Posición número 1 de ENISA del año 2007 (European Network and Information Security Agency).[5] Algunas de las recomendaciones que parecen más destacadas son:

- Las redes sociales deberían usar, siempre que sea posible, una información adaptada al contexto, con el objetivo de educar en tiempo real.
- Las campañas de concienciación deberían ir dirigidas también a los programadores de software, con el fin de favorecer prácticas y políticas de empresa que respeten la privacidad.
- Es necesario realizar un estudio atento de la regulación que pueda aplicarse a las redes y revisar o dar respuesta adecuada, como mínimo, a las siguientes cuestiones:
  - ¿Qué sucede con el contenido de un usuario que el proveedor de servicios borra porque lo considera *spam*?
  - ¿Qué sucede con las etiquetas o comentarios en las imágenes (*image-tagging*) colocados por terceros?
  - ¿Quién es responsable de los problemas de seguridad derivados de la actividad de los usuarios?
  - ¿Cómo se deberían comunicar a los usuarios las políticas de privacidad de terceros incluidos en la Red?
  - ¿Qué es un dato personal en una red social?
  - ¿Cuál es la posición legal del que suplanta un perfil?
  - ¿Se deberían proteger algunos datos de menores, como la localización?
- Se debería informar a los usuarios de lo que se hace con sus datos antes y después de cerrar la cuenta.
- El fenómeno de las redes se debería tratar de manera controlada y transparente, sin prohibir o desaconsejar, con campañas dirigidas a los menores, a los profesores y a los padres.

El tercer documento relevante es el *Working Paper* (n.º 163) del grupo de trabajo del artículo 29, sobre redes en línea, del 12 de junio del 2009.[6] Este documento avanza en la aplicación de la Directiva de Bases de Datos Personales en el ámbito de las redes sociales.

- Obligación de los proveedores de cumplir con la Directiva de protección de datos, e incluso la Directiva de e-privacidad, si ofrecen servicios de comunicaciones electrónicas.
- Obligación de los proveedores de informar de su identidad e indicar las diferentes finalidades con las que se tratan los datos personales de los usuarios.
- Se recomienda que sólo se puedan colgar imágenes e información de terceros con el consentimiento de los individuos en cuestión.

4. Adoptada en la XXXII Conferencia Internacional de Agencias de Protección de Datos y Privacidad en Estrasburgo, el 17 de octubre del 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*, n.º 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 línea].
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_es.pdf

- Los proveedores tendrían la obligación de advertir del derecho a la privacidad de los terceros.
- En el caso de datos sensibles, el consentimiento debería ser explícito, a menos que fuera un dato público. Si la red social incluye algún dato sensible en el perfil, debería hacer constar que es voluntario contestar. Las imágenes no serán un dato sensible, a menos que claramente sean usadas para revelar datos sensibles de los individuos.
- En cuanto a los datos de terceros, si los responsables de la Red informan a ese tercer no usuario acerca de la existencia de datos personales sobre él, un hipotético correo electrónico en el que se le invitara a ser usuario de la aquélla también podría vulnerar la prohibición del artículo 13.4 de la Directiva de e-privacidad, cuando se refiere al envío de mensajes electrónicos no solicitados para finalidades comerciales.
- Los socios terceros de la Red, que ofrecen servicios adicionales y que utilizan los datos personales en aquélla, deberían estar advertidos de que deben cumplir también las directivas mencionadas.

Incluso encontramos aquí una novedad interesante, más latente en las recomendaciones anteriores: la herramienta preferida para garantizar la privacidad es una buena seguridad y un funcionamiento garante de la privacidad (*privacy-friendly*) por defecto.

- Las redes sociales deberían prever estas características favorables a la privacidad sin coste añadido y restringiendo el acceso a los contactos seleccionados por el propio usuario. Cuando el acceso al perfil de información va más allá de los contactos seleccionados por el usuario, por ejemplo a todos los usuarios de la red social, o cuando el usuario debe aceptar contactos, independientemente de la relación que tengan con él, o si el dato no se puede indexar mediante un motor de búsqueda, nos encontraríamos con un acceso equivalente a público. Esto podría suponer la aplicación al usuario de la Directiva de protección de datos, por la que se le asimilaría a las responsabilidades que adquiere un responsable de una base de datos. Puesto que no se trataría ya de un ámbito doméstico, sino público, incluso la libertad de expresión debería ser matizada con el debido respeto al derecho a la privacidad. En esta línea, puesto que no concurre la excepción de uso doméstico, sería necesario proteger los derechos de terceros, sobre todo con relación a sus datos sensibles.
- El acceso restringido a los perfiles no debería ser posible con motores de búsqueda internos, con parámetros como la edad o la dirección. Además, las decisiones para extender el acceso no deberían estar implícitas.

Finalmente, destacamos la solución propuesta para el caso especial de los menores: la inclusión de medidas tecnológicas o *privacy enhancing technologies*:

- Educación escolar.
- No solicitar datos sensibles en el formulario de suscripción; no dirigir el marketing directo a los menores; obtener el consentimiento previo de los padres o tutores; y separar la comunidad de menores de la de adultos.
- Desarrollar *privacy enhancing technologies* (PET), por ejemplo, avisos en forma de *pop-up* o ventanas en ciertos momentos determinantes, o software de verificación de la edad.
- Código de conducta de los proveedores.

3. Riesgos no cubiertos por la protección de datos: el análisis de las redes sociales

3.1. Análisis de redes sociales (*social network analysis*)

El interés económico que genera la información personal contenida en las redes sociales ha provocado que crezcan proyectos comerciales a partir de la dirección de la Red, con socios terceros, y que aparezcan cada vez más herramientas de análisis de redes para particulares no asociados a la Red. Inicialmente, eran herramientas matemáticas sencillas ligadas a la teoría de *grafos* y a técnicas básicas sociológicas. En la actualidad se han vuelto cada vez más complejas, e incluyen interacción social y sistemas de reputación. Sus usuarios ya no son sólo los sociólogos o los estudiosos de las comunidades en línea, sino también particulares o profesionales que buscan colaboradores. Herramientas como VisoLink están, pues, centradas en el usuario y plantean retos para la privacidad.[7] Actualmente, las redes sirven tanto para el entretenimiento como para los profesionales, que participan en ellas. En el campo de la ciencia médica, por ejemplo, es vital poder intercambiar información sobre casos clínicos y metodologías en el

tiempo más corto posible, así como crear bases de datos históricas.[8]

Pero el riesgo no proviene sólo de motores de búsqueda externos de alcance cada vez más universal e incluso personalizado, el peligro para la privacidad radica también en la captura de información personal que el usuario involuntariamente ha puesto en la Red. Aquí no existe ninguna base de datos, ni siquiera una fuente estructurada o un dato personal explícito. A pesar de todo, una investigación llevada a cabo en una red social concreta ha revelado que el nombre del 72% de los usuarios y su nombre completo en un 30% de los casos podían deducirse fácilmente de los perfiles con técnicas estadísticas y heurísticas. Asimismo, la edad del 15% de los usuarios y, al menos, una escuela del 42% de los usuarios podían también deducirse de los datos colgados en la red social.[9]

3.2. La web 3.0, con los servicios de la web semántica, aumenta este riesgo para la privacidad

De hecho, con la creciente implantación de la tecnología de la web semántica, en la que los motores de búsqueda ya no se limitarán a las palabras clave sino también a sus significados, estos riesgos para la privacidad todavía serán más importantes. De hecho, las aplicaciones de web semántica añadirán al análisis de las redes sociales la posibilidad de extraer ontologías, es decir, mapas de significado, de las páginas web. De este modo, se obtendrá no sólo la ontología de conocimiento técnico elaborada por un experto, sino también una nueva estructura de significado basada en las relaciones en la comunidad en red, una semántica emergente.[10] La propia noción de dato personal queda aquí mortalmente debilitada, ya que la tecnología permite extraer datos personales, cada vez con más precisión y complejidad, de contextos desestructurados y sin capacidad, aparentemente, para identificar a nadie. La inclusión de la IP en el grupo de los datos personales sorprendió en su momento. Ahora nos enfrentamos al riesgo de que la capacidad de transformar en personal (identificable) un conjunto de datos aparentemente inocuos alcance niveles todavía más inverosímiles.

4. Las *privacy enhancing technologies* (PET) o tecnologías garantes de la privacidad

Un jurista suele considerar la tecnología como un riesgo para la privacidad. Esto puede ser efectivamente así, como se ha indicado antes. Ahora bien, estamos llegando a un nivel de posibilidades técnicas tan alto que se hace difícil incluso defender algunos derechos, como el de la privacidad, sin recurrir a contramedidas técnicas. Ésta es la idea de las PET o técnicas garantes: no sólo la tecnología no es el riesgo aquí, sino que también puede ser, si se dan las circunstancias propicias, una manera de proteger efectivamente el derecho. Los principios o recomendaciones a los legisladores apuntan tímidamente a esta posibilidad. Los ingenieros, a base de subvenciones públicas en proyectos de investigación europeos, ya han empezado a proponer prototipos que pronto serán adoptados por las redes sociales.[11] Vemos algunas de las posibilidades y capacidades de estos ingenios protectores.

4.1. La protección tecnológica contra los motores de búsqueda o minería de datos: el *privacy-preserving data mining* (P2DM)

La protección tecnológica de la privacidad es un área nueva, con menos de 10 años y con un planteamiento todavía muy teórico. En cambio, el *privacy-preserving data mining* (P2DM) es la excepción. El objetivo del P2DM es evitar, en la medida de lo posible, que se haga pública

7. FAN, L.; LI, B. (2008). «VisoLink: A User-Centric Social Relationship Mining». En: G. WANG [*et al.*] (eds.). *Lecture Notes in Artificial Intelligence*, n.º 5009, pág. 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». En: M. D. LYTRAS [*et al.*] (eds.). *WSKS 2008. Lecture Notes in Artificial Intelligence*, n.º 5288, pág. 22-30.
9. LAM, I.-F.; CHEN, K.-T.; CHEN, L.-J. (2008). «Involuntary Information Leakage in Social Network Services». En: K. MATSUURA; E. FUJISAKI (eds.). *IWSEC* (2008). *Lecture Notes in Computer Science*, n.º 5312, pág. 167-183.
10. MIKA, P. (2007), *Social Networks and the Semantic Web*. Nueva York: Springer.
11. Workshop on Privacy and Protection in Web-based Social Networks, 8 de junio del 2009, en el marco de la International Conference on Artificial Intelligence and Law. Barcelona, en prensa.

información personal de los usuarios de la Red cuando se analicen sus datos con finalidades estadísticas. Una herramienta de protección de la privacidad en las redes debe tener en cuenta no sólo los atributos de los usuarios, sino también sus relaciones.[12]

4.2. La protección tecnológica del acceso, de la identificación y de los sistemas de reputación

Las redes se basan en la confianza. Normalmente, la confianza se obtiene con el conocimiento del otro. Esto provoca que se considere habitualmente que cuanta más confianza hay, más datos personales identificables (PII, en inglés) del otro se desea tener y, por lo tanto, más riesgo para la privacidad.

Para romper esta lógica perversa, se ha pensado en primer lugar en mecanismos de autoidentificación o de reconocimiento, sin identificación. La idea es tener, al mismo tiempo, privacidad y confianza. Un modo de lograrlo es mediante el uso de seudónimos, que es una de las recomendaciones a los legisladores más habituales por parte de las agencias de protección de datos y grupos de expertos. Ahora bien, ésta tampoco es una solución definitiva: el análisis de la red social y la minería de datos pueden conseguir asociar estadísticamente un seudónimo a un usuario real. Por ello, los expertos recomiendan el uso de múltiples seudónimos. Existen soluciones técnicas para evitar el mal uso de los múltiples seudónimos.[13] En la misma línea, el proyecto europeo PRIME (Privacy and Identity Management for Europe) emplea credenciales privadas. Estas credenciales sirven de prueba de las autorizaciones, por ejemplo, ser mayor de edad, sin identificar al usuario. Sólo en caso de mal uso el anonimato podrá ser revocado.[14]

Como hemos indicado, las redes adoptan sistemas de reputación para garantizar la confianza. Ahora bien, los actuales sistemas de reputación generan perfiles del usuario que incluyen todos los contextos en los que éste ha estado interviniendo. Eso es frecuente en las redes de compraventa electrónica, en las que el tiempo, la frecuencia de la participación, la evaluación y el interés por ciertos productos pueden ser controlados. Además, los actores económicos suelen tener su seudónimo vinculado a un nombre real, lo que provoca que el perfil sea plenamente identificado. Otro riesgo en los sistemas de reputación se debe a los diferentes tipos de relaciones entre usuarios, como «amigo de». En el año 2006, miles de usuarios de Facebook protestaron por una utilidad denominada News Feed, que daba cuenta de la última información personal de los usuarios catalogados como amigos.[15] Para detener la avalancha de críticas, Facebook permitió a los usuarios disponer de algunas preferencias de privacidad. Más adelante, en noviembre del 2007, otro servicio de Facebook generó controversia: Beacon.[16] Beacon forma parte del sistema de alertas de Facebook, que sigue las actividades de los usuarios en la navegación por las páginas web de sus *partners*. Esta navegación era puesta a disposición de los amigos del usuario sin su consentimiento. De nuevo, las redes sociales han reaccionado ante las críticas, y han ofrecido a los usuarios mecanismos opcionales que permiten o no el acceso a su información personal (www.facebook.com, http://videntity.org).

Ahora bien, son necesarias estrategias más flexibles que permitan al usuario definir su política privada personal. La idea es que los usuarios indiquen quiénes están autorizados a acceder a su página personal, incluso si no son usuarios conectados con una relación de amistad.[17] Una opción es mediante un control de acceso por parte del

12. WANG, D.-W.; LIAU, C.-L.; HSU, T.-S. (2006). «A GrC-Based Approach to Social Network Data Protection». En: S. GRECO [*et al.*] (eds.). *RSCTC 2006. Lecture Notes in Artificial Intelligence*, n.º 4259, pág. 438-447.
13. SEIGNEUR, J. M. (2009). «Social Trust of Virtual Identities». En: J. GOLBECK (ed.). *Computing with Social Trust*, Londres: Springer. Human-Computer Interaction Series.
14. HANSEN, M. (2008). «Marrying Transparency Tools with User-Controlled Identity Management». En: 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, pág. 199-200. Boston: Springer.
15. CHEN, L. (octubre, 2006). «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

propio usuario,[18] o mediante la colaboración de un grupo de usuarios seleccionados, o sin un nódulo central.[19] Dicho esto, el control de acceso no es la única manera de preservar la privacidad en las redes sociales. Es necesario plantear otros sistemas de reputación garantes de la privacidad desde una óptica más general.

4.3. Sistemas de reputación garantes de la privacidad no basados en el acceso

Ya hemos indicado que las recomendaciones de las agencias de protección de datos, en el sentido de usar seudónimos, deberían traducirse en una multiplicidad de seudónimos. También hemos señalado que es necesario evitar el mal uso de éstos. Ahora debemos añadir que se puede obtener un sistema de reputación fiable con valoraciones de los seudónimos en diferentes contextos. Este esquema ha sido, incluso, propuesto para redes de P2P con seudónimos.[20] Se dispone de unos puntos de reputación (*e-cash*). Un usuario honesto puede cambiar su seudónimo conservando su reputación. En cambio, un usuario deshonesto no podrá borrar su cuenta de puntos, ni siquiera cambiando de seudónimo.

4.4. Tecnología para la transparencia, el contexto y la finalidad

Las tecnologías tradicionales garantes de la privacidad han buscado la anonimización, la seudoanonimización y la autenticación. Parece existir una tendencia que favorece actualmente las PET más centradas en la transparencia. En todo caso, son estrategias complementarias. Seguramente, la implantación progresiva de la normativa europea sobre protección de datos, muy centrada en el control de la información y en la finalidad, puede explicar, cuando menos, parcialmente, este nuevo enfoque.

Las tecnologías de la transparencia deben garantizar que el flujo de información sea visible y deje rastro. Y se pretende que lo hagan de una manera amplia, que afecten tanto a las políticas de privacidad como al procesamiento de los datos, a los servicios ofrecidos, al software utilizado, a los colaboradores y a la confianza, así como a posibles problemas de seguridad. Las herramientas de transparencia, por sí solas, no solucionan los riesgos para la privacidad. Sólo su combinación con la gestión de la identidad y los sistemas de reputación puede ofrecer garantías para la privacidad.

Una posibilidad extrema es la de las TET (*transparency enhancing technologies*), que pretende anticipar un posible perfil que se pueda deducir de los datos de un particular. La idea central es disponer de suficiente información para ser capaz de construir un perfil contrario a lo que se deduce de la información disponible. El uso más habitual de la tecnología de la transparencia, sin embargo, es poder saber en todo momento qué dato personal se ha proporcionado al sistema, con el fin de acceder a él, alterarlo o borrarlo. En el proyecto europeo PRIME, el buscador de datos o Data Track cumple esta función. Antes de dar información personal se puede consultar la actividad de los colaboradores y la política de privacidad. Esta información sirve también para pedir a los responsables de los datos si han actuado correctamente o para investigar riesgos detectados en anteriores utilizaciones del buscador de datos.

Conclusiones

La protección de la privacidad en las redes sociales no es la adecuada. Hay varias razones que coinciden en esta situación delicada:

- El marco regulador es inexistente o muy limitado. Sólo la regulación sobre la protección de las bases de datos

17. CARMINATI B.; FERRARI, E. (2008). «Privacy-Aware Collaborative Access Control in Web-Based Social Networks». En: V. ATLURI (ed.). *Lecture Notes in Computer Science*, n.º 5094, pág. 81-96.
18. CARMINATI B.; FERRARI, E.; PEREGO, A. (2007). «Private relationships in social networks». En: *ICDE 2007 Workshops Proceedings*. Los Alamitos: IEEE CS Press. Pág. 163-171.
19. DOMINGO-FERRER, J. (2007). «A Public-Key Protocol for Social Networks with Private Relationships». En: V. TORRA, Y. NARUKAWA; Y. YOSHIDA (eds.). *MDAI 2007. Lecture Notes in Artificial Intelligence*, n.º 4617, pág. 373-379.
20. ANDROULAKI, E.; CHOI, S. G.; BELLOVIN, S. M.; MALKIN, T. «Reputation Systems for Anonymous Networks». En: N. BORISOV; I. GOLDBERG (eds.). *PETS 2008. Lecture Notes in Computer Science*, n.º 5134, pág. 202-218.

personales configura un cuerpo destacado. Ahora bien, su plena vigencia se centra en los países europeos. Existe, no obstante, una tarea muy notable de las agencias de protección de datos, y de los grupos de trabajo próximos a éstas, que va concretando medidas y recomendaciones útiles. En este sentido, se está intentando llegar a un estándar internacional de privacidad en las redes sociales que podría resultar un primer marco regulador de referencia en la materia. Ahora bien, la reducción de toda la problemática a la protección de las bases de datos excluye aspectos relevantes de la protección de la privacidad en las redes sociales que sería preciso no olvidar.

- La tecnología de protección de la privacidad aparece por primera vez, tímidamente, en algunas recomendaciones. La fragilidad es doble: por un lado, existe una fundamentación jurídica de la tecnología como garante de derechos. Más bien al contrario, la tecnología es vista como fuente de riesgos para los derechos. Una posible fundamentación podría derivar del principio de proporcionalidad, que rige las limitaciones de derechos. En resumen, la necesidad de una restricción de derechos se valora por la imposibilidad de llevar a cabo una finalidad legítima, como podría ser la gestión de una red social, con una menor afectación a los derechos. Pues bien, si las PET o tecnologías garantes de la privacidad fueran de alcance público, se podrían cuestionar las restricciones de la privacidad como medidas desproporcionadas, por innecesarias. Por otro lado, las PET tienen muchas dificultades para pasar del aspecto teórico de los proyectos europeos, que es en el que aparecen, al posterior desarrollo y aplicación comercial. No parece existir impulso público ni conciencia particular de esta delicada situación y, por ahora, son considerados por la industria como un gasto extra no impuesto por ninguna ley, ni sancionado por ninguna agencia.
- Las redes sociales son un campo especialmente vulnerable para la privacidad. Pero no son el único: la computación ubicua, las etiquetas RFID y la robótica, según nuestros limitados conocimientos, son también retos muy difíciles. Una posible aproximación, más anglosajona, consiste en hacer que la industria tenga interés económico en desarrollar herramientas que incorporen una versión «amiga de la privacidad». El interés de esta propuesta consiste en que las soluciones son más sencillas y más baratas si se incorporan ya en el diseño del sistema o programa que si se intenta añadir *a posteriori* un «paquete» adicional de PET. Quizá por ello, las propias PET van incorporando otras opciones además de las tradicionales basadas en el anonimato, los seudónimos y las autenticaciones. Parece dibujarse, no obstante, un riesgo: la negociación de las facultades o derechos entre el usuario y la red social, o entre usuarios, a cambio de beneficios, transforma los derechos fundamentales en opciones individuales. Tal vez la privacidad puede acabar de diluirse en este mercado de intercambios o de concesiones. Por esta razón queremos destacar el dictamen, en el marco de las etiquetas RFID, del supervisor europeo de protección de datos que, por desgracia, todavía no parece haber llegado a las propuestas de las agencias sobre redes sociales: la previsión de las medidas tecnológicas garantes de la privacidad en el mismo momento del diseño de la herramienta.[21] Éste es un reto no sólo para los ingenieros de las PET, que deberán pensar «en tiempo real» y en el contexto específico de un producto comercial; también lo es para el derecho, si no nos queremos quedar, en el mejor de los casos, con un listado de principios generales. La previsión de estándares técnicos protectores de la privacidad podría ser la última oportunidad para la regulación, entendida ésta como una competición entre los intereses comerciales particulares y los intereses generales, como es el caso de la privacidad. La redefinición de la privacidad se realizará, presumiblemente, no en grandes definiciones, sino en pequeñas y constantes redefiniciones de técnicas garantes en ámbitos como las redes sociales. Si no estamos atentos, el derecho a la privacidad puede acabar siendo sólo un «derecho ficción».

21. Dictamen del Supervisor Europeo de Protección de Datos relativo a la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «La identificación por radiofrecuencia (RFID) en Europa: Pasos hacia un marco político», documento COM (2007) 96, (2008/C101/01), donde habla de la necesidad «de intimidad mediante el diseño».

Referencias

ANDROULAKI, E.; CHOI, S. G.; BELLOVIN, S. M.; MALKIN, T. «Reputation Systems for Anonymous Networks». En: N. BORISOV; I. GOLDBERG (eds.). *PETS 2008, Lecture Notes in Computer Science*. N.º 5134, pág. 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». En: V. ATLURI (ed.). *Lecture Notes in Computer Science*. N.º 5094, pág. 81-96.

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

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

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

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

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (2009). *Dictamen 5/2009 sobre las redes sociales en línea*. [informe en línea]. ‹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». En: 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, pág. 199-200. Boston: Springer

HOGBEN, G. (ed.) (octubre, 2007). «Security Issues and Recommendations for Online Social Networks». *Enisa Position Paper*. N.º 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 (Memorandum de Roma)». En: *43.ª reunión* (3-4 de marzo del 2008: Roma) [informe en línea]. Informe n.º 675.36.5. IWGDPT. ‹http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491›

LAM, I.-F., CHEN, K.-T. y CHEN, L.-J. (2008). «Involuntary Information Leakage in Social Network Services». En: K. MATSUURA; E. FUJISAKI (eds.). IWSEC (2008). *Lecture Notes in Computer Science*. N.º 5312, pág. 167-183.

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

SEIGNEUR, J. M. (2009). «Social Trust of Virtual Identities». En: J. GOLBECK (ed.). *Computing with Social Trust*. Londres: Springer. 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». En: M. D. LYTRAS [*et al.*] (eds.). *WSKS 2008*, *Lecture Notes in Artificial Intelligence*. N.º. 5288, pág. 22-30.

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

Cita recomendada

ROIG, Antoni (2009). «E-privacidad y redes sociales». En: «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 9. UOC. [Fecha de consulta: dd/mm/aa].

‹http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_roig/n9_roig_esp›

ISSN 1699-8154

Sobre el autor

Antoni Roig
antoni.roig@uab.cat

El Dr. Antoni Roig es profesor de Derecho constitucional en la Facultad de Derecho de la UAB. Ha sido investigador en proyectos nacionales y europeos. Cuenta con publicaciones en las áreas de fuentes del derecho, derecho europeo, bases de datos, tecnología y libertad de expresión y privacidad de ciudadanos y trabajadores. Sus últimas publicaciones se han centrado en la privacidad y el gobierno electrónico.

Cuenta con un doctorado en Derecho por la UAB y ha realizado estudios post-doctorales en las Universidades Cattolica di Milano (Milán, 1996-1997) y Università degli Studi di Firenze (Florencia, 1997). En la actualidad, participa en un curso de ingeniería técnica informática en la Universitat Oberta de Catalunya.

IDT, Instituto de Derecho y Tecnología
Universidad Autónoma de Barcelona
08193 Bellaterra (Barcelona), España