Seguridad en Redes Sociales: problemas, tendencias y retos futuros

Lorena González-Manzano
Univ. Carlos III de Madrid
Leganés, España
lgmanzan@inf.uc3m.es

Ana I. González-Tablas
Univ. Carlos III de Madrid
Leganés, España
aigonzal@inf.uc3m.es

José M. de Fuentes
Univ. Carlos III de Madrid
Leganés, España
jfuentes@inf.uc3m.es

Arturo Ribagorda
Univ. Carlos III de Madrid
Leganés, España
arturo@inf.uc3m.es

***Resumen*—El abrumador crecimiento de las Redes Sociales (RSs) junto con su gran utilización, estimulan su constante investigación y mejora. Sin embargo, el uso de las RSs no está exento de problemas de seguridad y, en concreto, de privacidad. De hecho, es aquí donde este trabajo contribuye. En base a las recientes investigaciones y tendencias, se presentan un total de diez problemas asociados con la privacidad en las RSs. Además, cada problema es acompañado de directrices que pretenden ser la base de futuras investigaciones y desarrollos. Finalmente, se analiza de forma global la dificultad técnica de abordar estos problemas, así como su alcance en las RS.**

***Palabras Clave*—Redes sociales, privacidad, seguridad.**

I. Introducción

La gran expansión y desarrollo de las Redes Sociales (RSs) es un hecho indiscutible. Por ejemplo, Facebook ha superado los 800.000 millones de usuarios[1]. Sin embargo, tampoco es cuestionable la cantidad de problemas de seguridad que estos sistemas plantean. En cualquier medio de comunicación, día tras día, aparecen casos que atentan contra la seguridad de los usuarios de las RSs y, en concreto, contra su privacidad. Una muestra de ello es el desarrollo de un programa que permite rastrear a los usuarios por medio de, entre otras cosas, la información publicada en las RSs[2].

Es cierto que la privacidad pasa desapercibida para muchos usuarios. Estudios como el realizado por J. Becker *et al.*, indican que gran parte de los usuarios de Facebook nunca ha hecho uso de los mecanismos de privacidad proporcionados (1). Asimismo, Acquisti *et al.* estudiaron que incluso los usuarios de Facebook que eran conscientes de los problemas de privacidad que se producían, continuaban utilizándolo (2). En cambio, un reciente estudio realizado por R. Dey *et al.* muestra un incremento en la precupación por la privacidad en las RSs. En dicho estudio, se indica que el diseño de la página de privacidad es un factor clave en el desarrollo de estos sistemas (3). De hecho, con independencia de las investigaciones realizadas y las preferencias de los usuarios, la Declaración Universal de los Derechos Humanos establece el derecho a que nadie ha de ser objeto de injerencias arbitrarias en su vida privada, familiar o correspondencia[3]. Además, el derecho a la intimidad y la privacidad personal se recoge en la Constitución de muchos países (e.j. Constitución española (4)) y se desarrolla en leyes de protección de datos de carácter personal. Por tanto, la privacidad ha de preservarse.

Las RSs se pueden definir, a grandes rasgos, como un grafo en el que los nodos son los usuarios y las aristas las relaciones, las cuales pueden ser de muy diversos tipos, por ejemplo, unidireccionales, bidireccionales, directas o indirectas, entre otras (Figura 1). Además, cada usuario tiene asociado un conjunto de datos que comparte con los usuarios con los que ha establecido alguna relación, es decir, con sus contactos. Por consiguiente, a grandes rasgos, las entidades involucradas en las RSs, que tienen entidad propia fuera de las mismas, son los datos y los usuarios.

Debido a la gestión de grandes cantidades de datos y usuarios, aparecen retos a los que profesionales y científicos han de enfrentarse, siendo éste el punto de partida de este trabajo. Es posible indicar la existencia de propuestas que contribuyen en la identificación de riesgos y posibles contramedidas (5). En cambio, la contribución principal presentada en este artículo consiste en la identificación y descripción de los problemas de privacidad que, prestando atención a las recientes investigaciones y tendencias, subyacen tras las RSs. Además, la descripción de cada problema es acompañada de un conjunto de directrices que pretenden ser la base de futuras investigaciones y desarrollos. En último lugar, se presenta una breve discusión sobre los problemas más controvertidos y un análisis que permite determinar aquellos a los que es necesario prestar mayor atención en función de las entidades afectadas: usuarios y datos. En conclusión, el presente artículo realiza un estudio sobre la privacidad en las RSs desde una perspectiva general, aportando una visión hasta ahora inexistente. Asimismo, pretende ser un complemento de gran ayuda para, posteriormente, profundizar en el estudio de los distintos problemas identificados.

La estructura del documento es la siguiente. En la Sección II se presentan trabajos relacionados con el presentado en este documento. Posteriormente, en la Sección III se describen los problemas de privacidad identificados en las RSs. En la Section IV se realiza una breve discusión sobre los problemas identificados. Finalmente, en la Sección V se presentan las conclusiones.

[1]http://www.internetworldstats.com/facebook.htm, último acceso Abril 2013

[2]http://www.guardian.co.uk/world/2013/feb/10/software-tracks-social-media-defence, último acceso Abril 2013

[3]http://www.un.org/es/documents/udhr/, último acceso Abril 2013

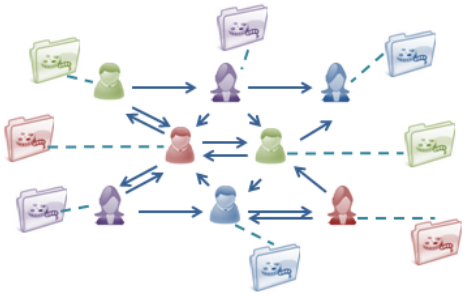

Figura 1. Definición de una RS

II. Antecedentes

Considerando el abrumador crecimiento de las RSs, numerosas propuestas estudian la seguridad de estos sistemas. Por un lado, la investigación de riesgos y medidas de prevención es un tema de notable interés. R. Ajami *et al.* (5) realizan un análisis de los riesgos presentes en las RSs, entre los que destacan: los *riesgos de privacidad*, tales como la falta de herramientas que permitan controlar de una manera práctica y sencilla la privacidad; los *riesgos de seguridad*, como los producidos por la ingeniería social; y los *riesgos de anonimato*, como los provocados por las revelaciones de datos sin consentimiento previo. Además, se indican algunos controles para mitigar los riesgos identificados. Asimismo, A. Ho *et al.* identifican riesgos de las RSs, pero desde el punto de vista de la seguridad, los perfiles y la reputación y la credibilidad (6). Siguiendo una línea similar, en (7) se presenta un estudio sobre las amenazas existentes en las RSs, como son los virus o el spam. Además, se incluyen un conjunto de recomendaciones de seguridad para los proveedores de información, tanto a nivel teórico, por ejemplo que se maximicen las posibilidades de detectar abusos, como a nivel técnico, por ejemplo la necesidad de que los usuarios tengan que consentir ser etiquetados en determinados contenidos.

Desde otro punto de vista, C. Zhang *et al.* analizan problemas de privacidad y seguridad en el diseño de RSs (8). Por un lado, se identifican las características que una RS ha de proporcionar, como por ejemplo la posibilidad de que un usuario pueda darse de baja o de alta. Por otro lado, se estudian los retos a los que se enfrentan las RSs en relación con los principios de seguridad, incluyendo confidencialidad, integridad y disponibilidad.

Por último, pero no menos importante, autores como H. Gao *et al.* describen un conjunto de mecanismos de defensa contra las posibles infracciones que pueden ocurrir en las RSs (9). En concreto, se identifican infracciones producidas por proveedores de servicio, por aplicaciones de terceros y por los propios usuarios. Igualmente, enfocándose en el establecimiento de contramedidas, pero en el área del control de acceso, se desarrolla (10). En esta propuesta se enumeran requisitos necesarios para mejorar el control de acceso en las RSs. Entre los controles propuestos cabe destacar la necesidad de indicar explícitamente la información que cada usuario está desvelando.

Por todo lo comentado, los trabajos identificados se enfocan en aspectos concretos de la privacidad, como son los riesgos antes posibles ataques o los problemas de control de acceso. Sin embargo, este artículo proporciona el lector una visión a alto nivel de los problemas de privacidad en las RSs, de modo que sirve como complemento de otros estudios realizados que se especializan en un problema concreto.

III. Problemas de privacidad en RSs

Paralelamente a la creación y difusión de las RSs, así como a su persistente mejora y preocupación por la privacidad, gran cantidad de desarrollos e investigaciones se están llevando a cabo. Prestando atención a tales propuestas en las siguientes secciones se describen un total de diez problemas relacionados con la privacidad, así como directrices que pretenden ser la base de futuras contribuciones.

III-A. Sybil nodes

El término *sybil nodes*[4] hace referencia a la creación de nodos falsos, es decir, nodos deshonestos. En una red social se pueden clasificar dos tipos de nodos: honestos, que se corresponden con usuarios reales que se registran en la red con el fin de hacer uso de la misma de forma apropiada; y deshonestos, que se corresponden con usuarios con perfiles falsos que se registran para fines distintos a los proporcionados por las RSs, no previstos y por tanto ilegítimos. Este hecho es ampliamente conocido en el contexto de las RSs, e.g. falsificación de perfiles de cantantes o futbolistas, y plantea serios problemas de privacidad. En concreto, los perfiles falsos pueden utilizarse para conseguir información de un modo sencillo y sin necesidad de realizar actividades ilícitas.

Debido al peligro de los *sybil nodes*, distintas propuestas buscan su identificación dentro de una RS. De forma general, la idea subyacente se basa en asumir que el grafo de relaciones creado por los nodos honestos tendrá más relaciones que las producidas por los nodos deshonestos (11). De hecho, se trabaja bajo la premisa de que los nodos deshonestos no son capaces de establecer un gran número de vínculos. Una de las últimas propuestas consiste en la búsqueda de caminos aleatorios desde un determinado nodo, de modo que los caminos desde un nodo deshonesto deberán ser de menor longitud que los creados desde nodos honestos (12). Sin embargo, gran parte de las soluciones presentadas son vulnerables a *sybil attacks* (13) y, por ello, se requieren nuevas investigaciones.

Considerando futuras tendencias, y como indica (14), una nueva posibilidad en la búsqueda de *sybil nodes* es el seguimiento de la actividad de los usuarios y no el análisis de la estructura de la RS. La identificación de nodos deshonestos parte de la idea de que, con mayor frecuencia, los usuarios escriben mensajes, visualizan fotos o realizan cualquier tipo de actividad con un conjunto determinado de contactos, los cuales se clasifican como nodos honestos.

[4]El término sybil (sibila en español) fue establecido tras la creación del libro "Sybil" escrito por F. R. Schreiber en 1973, en el que se narra la historia de una mujer con trastorno de identidad disociativo.

III-B. Co-propiedad

Las RSs hacen uso de multitud de datos y, en ocasiones, pueden involucrar a más de una persona. Por ejemplo, una foto puede ser subida por un determinado usuario pero si hay más usuarios en ella, los cuales son etiquetados, pasan a ser co-propietarios de la misma (15). El término co-propiedad se asocia con cualquier dato, ya sea foto, mensaje, video, etc., en el que se involucre a otros usuarios además del propietario original del mismo.

Varias propuestas han sido desarrolladas en relación con la co-propiedad, siendo A. Squicciarini una de las autoras más destacadas. Una de sus primeras propuestas se basa la creación de subastas en las que los usuarios deciden colectivamente subir o no un determinado objeto (15). Desde una perspectiva similar, en (16), se presenta la gestión de la co-propiedad mediante una función que intenta maximizar la utilidad social. Sin embargo, la mayoría de las propuestas se basan en esquemas de voto para establecer las preferencias de control de acceso (equivalentes a políticas). Todos los usuarios, propietarios y co-propietarios, votan unas determinadas preferencias y, tras realizarse unos cálculos, se establecen las preferencias a aplicar (17; 18; 19; 20). Todas estas propuestas presentan un punto común de fallo, las preferencias se realizan en base a un consenso entre todos los usuarios pero es posible que la privacidad de algunos de ellos se viole. En otras palabras, es posible que prevalezcan unas preferencias sobre otras y, por ello, algunas preferencias no sean consideradas. De hecho, la propuesta presentada por K. Thomas *et al.*, aunque sencilla, es la única que consigue preservar la privacidad de todos los usuarios (21). En concreto, se basa en calcular la intersección de las preferencias de todos los usuarios. No obstante, existe una alta probabilidad de que no todos los usuarios establezcan unas preferencias comunes y, por tanto no se llegue a un consenso. De hecho, dadas las limitaciones de la propuesta, lo interesante es buscar un balance entre la utilidad y la privacidad.

Por todo lo comentado, el análisis de la co-propiedad ha de ser investigado en mayor profundidad, buscando soluciones que preserven la privacidad de todos los usuarios. Sin embargo, a diferencia de la propuesta de K. Thomas *et al.* donde es posible que no se encuentren preferencias que intersecionen, se podrían utilizar técnicas para el procesado y ocultación de elementos. Por ejemplo, el procesado de imágenes puede ser un campo de gran interés (22), de forma que un mismo elemento se muestre de manera distinta a cada usuario en función de las preferencias establecidas.

III-C. Trazabilidad e inferencia de datos

El crecimiento de la hiper-conectividad, la necesidad de que todo el mundo esté conectado y en persistente contacto, es otro de los problemas que plantean serios riesgos para la seguridad. Propuestas como (23) muestran la posibilidad de obtener datos personales a través de la información presente en las RSs. Asimismo y siendo un fenómeno de gran relevancia, Raytheon Company[1] ha desarrollado recientemente un sistema para, haciendo uso de la información expuesta en las RSs, poder rastrear a los usuarios y predecir desplazamientos y comportamientos.

Por otro lado, ofreciendo un visión positiva sobre la trazabilidad y la inferencia de datos, E. Lalas propone la identificación de las acciones de los usuarios para poder realizar reclamaciones ante determinadas situaciones (24). En concreto, se pretende conocer qué usuarios, con los que se ha establecido una relación de confianza, dejan de actuar adecuadamente y, en consecuencia, dejan de ser confiables.

Una vez presentadas las dos facetas (negativa y positiva) que presentan la trazabilidad y la inferencia de datos y, a la vista de los grandes desarrollos realizados, es complejo identificar futuras líneas de trabajo. No obstante, de forma similar a (24), es conveniente subrayar la necesidad de crear técnicas que identifiquen comportamientos inadecuados o ilegales a la luz de alguna ley de protección de datos, e.g. copiar una foto de un perfil para subirla en otro, así como su posterior notificación a los usuarios afectados.

III-D. Privacidad en la localización

RSs como Facebook Places o FourSquare, basadas en localizar a usuarios, plantean serios problemas en relación con la privacidad. Por un lado, aplicaciones como las conocidas "*CheckIn*" hacen uso de la localización para proporcionar ventajas como pueden ser descuentos al tomar un café. En cambio, el hecho de estar constantemente localizado implica una pérdida de privacidad por parte de los usuarios. Por ejemplo, la localización podría utilizarse para fines ilícitos como es la identificación de un usuario fuera de su hogar y la posibilidad de perpetrar un robo. Es cierto que algunos países imponen a sus operadores de telecomunicaciones la adopción de estrictas medidas de seguridad en la custodia y el tratamiento de estos datos, pero aún queda mucho por hacer.

Por este motivo, numerosas propuestas se enfocan en la protección de la privacidad en la localización. Las técnicas son muy diversas: *position dummies*, mandar gran cantidad de mensajes de forma que sólo algunos de ellos sean verdaderos; *mix-zones*, establecer zonas en las que las identidades de los usuarios se mezclan y no es posible diferenciarlos; *K-anonymity*, establecer K usuarios indistinguibles; *ofuscación*, ofrecer información imprecisa, es decir, con menor granularidad; o *propuestas criptográficas*, utilizar cifrado en las comunicaciones de la localización. Recientemente se han realizado nuevas propuestas, como (12) en la que se realiza una combinación entre el anonimato en la localización y el envío de mensajes entre los cuales hay un porcentaje de mensajes falsos, o (25), en la que se propone un esquema dinámico de *K-anonymity*. Sin embargo, todas las contribuciones toman como punto de partida, de un modo u otro, las técnicas anteriormente descritas.

Como última observación, en base a los nuevos desarrollos, una de las futuras tendencias asociadas con la privacidad en la localización puede relacionarse con la esteganografía. Esta técnica criptográfica se basa en la ocultación de la información de modo que pase inadvertida, lo cual es el objetivo buscado en la privacidad de la localización, enviar la localización de los

usuarios sin que ésta pueda ser identificada. Por este motivo, la esteganografía es una futura línea de investigación en la que, actualmente, pocos autores han contribuido (26; 27).

III-E. Interoperabilidad

En la literatura este problema recibe el nombre de *Wall Garden Problem* (28), es decir, las RSs se visualizan como jardines cerrados de los que es difícil salir y pasar de unos a otros. En la actualidad hay multitud de RSs y, todas ellas, proporcionan un sinfín de servicios. Por este motivo, los usuarios tienen que registrarse en distintas RSs y gestionar gran cantidad de datos, en muchos casos los mismos datos en varias RSs. Atendiendo a los recientes avances, cada vez más se intentan realizar desarrollos que permitan compartir información entre distintas RSs. Por ejemplo, en Facebook es posible visualizar los *tweets* escritos en Twitter. No obstante, existen otros muchos datos, como pueden ser los contactos, el perfil personal, las políticas de control de acceso, etc., que no son interoperables y, lo que es más, pocos han sido los autores que han estudiado este hecho (29; 30). En otras palabras, queda mucho por hacer para conseguir interoperabilidad y mas aún cuando a esta necesidad se le suma el requisito de privacidad.

En base a las propuestas actuales, algunas de ellas pueden ser utilizadas para conseguir interoperabilidad. Como punto de partida se pueden mencionar distintos estándares, como son FOAF[5] o XFN[6], así como ontologías de datos especialmente desarrolladas para este fin (31). Asimismo, una forma de conseguir interoperabilidad es haciendo uso de un esquema similar al modelo de autorización *push model*[7], de modo que los datos y la gestión del acceso se descentralice. En este modelo los datos se solicitan en una determinada entidad que, tras verificar la satisfacción de las políticas de control de acceso apropiadas, entrega un elemento (ej. certificado o token) que prueba que el usuario que realiza la solicitud tiene o no acceso a los datos solicitados. Posteriormente, el usuario va a otra entidad, entrega el elemento obtenido y si la verificación es correcta, se le proporciona el dato solicitado. En relación con este esquema se identifican distintas contribuciones (32; 33). Sin embargo, (29) es el único trabajo cuya contribución principal es el desarrollo de un protocolo para conseguir la interoperabilidad de datos personales, de recursos como son fotos, mensajes, etc., y de políticas de control de acceso.

Partiendo de la necesidad de crear RSs interoperables, una futura línea de desarrollo que, tal y como se ha comentado, es la base de las propuestas actuales, es la descentralización. Conseguir que todo tipo de datos estén descentralizados, de forma que únicamente haya que especificar el lugar en el que se almacenan, es una de las claves que pueden facilitar la creación de propuestas enfocadas a la interoperabilidad.

[5]http://www.foaf-project.org/, último acceso Abril 2013
[6]http://gmpg.org/xfn/, último acceso Abril 2013
[7]http://tools.ietf.org/html/rfc2904page-7, último acceso Abril 2013

III-F. Control de los datos almacenados

Las RSs almacenan todos los datos que son subidos a cada una de ellas, de modo que los proveedores de servicio tienen control sobre todo tipo de datos. Por un lado, dichos proveedores proporcionan todos los servicios conforme a la RS a la que se vinculan. No obstante, los datos también pueden utilizarse para otros propósitos, como por ejemplo fines comerciales. Este tipo de servidores en los que se almacenan grandes cantidades de información y en los que, además de ofrecer servicios, los datos se utilizan para otros propósitos, se les conoce con el nombre de servidores honestos pero curiosos (*honest-but-curious servers*) (34).

La forma habitual de enfrentarse a este problema es utilizar técnicas criptográficas. El procedimiento general se basa en el uso de pares de claves públicas-privadas y variados algoritmos criptográficos para cifrar los datos con anterioridad a ser almacenados en las RSs (35; 36; 37). También se han propuesto esquemas híbridos en los que los datos se cifran simétricamente y la criptografía asimétrica se aplica en la adquisición y el descifrado de los datos (38). Además, la utilización de criptografía no solo requiere la creación de claves, sino también la distribución de las mismas entre los usuarios adecuados. Sin embargo, en un entorno como son las RSs, en el que hay gran cantidad de usuarios involucrados, la gestión de las claves puede convertirse en un proceso complejo e incluso, inmanejable.

Como conclusión, es importante incidir en la utilidad de la criptografía para proteger la información que se almacena en los servidores. No obstante, es necesario desarrollar esquemas de gestión de claves que reduzcan, en la medida de lo posible, la cantidad de intercambios de claves que se han de realizar. Además, por otro lado y siguiendo la misma línea indicada en el problema de la localización, la utilización de la esteganografía se subraya como futura línea de desarrollo. Indicado por A Nourian *et al.* en (39), esta novedosa técnica requiere mayor espacio de almacenamiento pero, en la actualidad, este hecho dista de ser un problema (40) y, por tanto, es una técnica sujeta a estudio.

III-G. Control de acceso simplificado

Como se ha mencionado en numerosas ocasiones, las RSs hacen uso de una gran cantidad de datos cuya gestión puede convertirse en un proceso complejo y, a su vez, incómodo. Por este motivo se plantea necesario el desarrollo de sistemas que permitan aliviar dicho trabajo.

La gestión del control de acceso se basa, principalmente, en el establecimiento de políticas de control de acceso en relación con los datos disponibles en la RS y los usuarios a los que se les desea otorgar acceso. Distintas propuestas se han desarrollado para simplificar esta tarea. *Social Circles* propone un procedimiento, basado en el agrupamiento de usuarios vinculados con un usuario dado, para simplificar la gestión de las listas de amistad (41). Otros trabajos proponen obtener automáticamente las políticas de los usuarios basándose, por ejemplo, en los atributos de los contenidos que se suben a las RSs (42).

La gestión del control de acceso se puede simplificar de múltiples formas, pero la automatización es la técnica más habitual, pudiendo realizarse distintas consideraciones al respecto. Por un lado, es posible automatizar el establecimiento de las políticas de control de acceso o la creación de grupos pero, por el hecho de ser un procedimiento automático, es susceptible de errores. Por otro lado, la automatización reduce la granularidad con la que un usuario puede gestionar sus datos, es decir, existe una alta probabilidad de que preferencias muy concretas no se lleguen a establecer. Por estos motivos, la participación del usuario en la gestión del acceso es fundamental. En relación a esta cuestión y prestando atención a modelos de control de acceso existentes (43; 44), en lugar de asociar una política a cada dato, los usuarios podrían crear un conjunto ("*pool*") de políticas. Posteriormente, en vez de evaluar una política concreta asociada a un dato, se evalúan todas las políticas creadas y se otorga o no acceso en función del resultado de la evaluación.

III-H. Anonimato de usuarios

Las RSs permiten la comunicación de todo tipo de usuarios pero, para ello, es necesario registrarse. Sin embargo, en determinadas ocasiones los usuarios pueden desear no identificarse, es decir, permanecer en el anonimato. Por ejemplo, suponiendo un grupo de usuarios que crea un perfil para ayudar a minusválidos, facilitándoles ayuda económicas y posibilidades de inserción laboral, es posible que los usuarios que deseen acceder a este perfil no quieran ser identificados.

A pesar de la problemática de la situación, pocas son las propuestas relacionadas a este respecto. Por un lado, hay propuestas basadas en el anonimato de los datos, como las mencionadas en la Sección III-D, basadas en seudónimos o en la ofuscación de la información. Otros trabajos, al contrario, se basan en proporcionar anonimato en las comunicaciones como son Pisces (45) o Gossple (46). El primero de ellos se enfoca en la gestión de relaciones de confianza entre los usuarios. En cambio, en Gossple se asocia a cada usuario un conjunto anónimo de usuarios con los mismos intereses con los que poder interactuar.

Observando la gran cantidad de atributos de los usuarios de una RS, por ejemplo, edad, estudios o cualquier otra información del perfil, se plantea una nueva línea de investigación, el uso de credenciales anónimas (47). Es innegable que el uso de esta técnica implica grandes capacidades cómputo (47), pero las constantes mejoras en los algoritmos revelan la posibilidad de utilizarlos (48).

III-I. Derecho al olvido

Una cuestión que muy recientemente ha suscitado interés es la siguiente ¿Qué ocurre con los datos que, por algún motivo, dejan de ser utilizados? En relación con las RSs se pueden diferenciar dos situaciones, la baja voluntaria y el fallecimiento de un usuario. En ambos casos la problemática subyacente es similar, es decir, hay que determinar qué datos han de ser eliminados y cómo se ha de realizar la eliminación.

Para hacer frente a estos problemas, muy recientemente, en Enero de 2012, la Unión Europea propuso el "Derecho a ser olvidado" ("*The right to be forgotten*") (40). En líneas generales, este derecho establece que los proveedores de servicio han de eliminar los datos que los usuarios soliciten, así como incluir la opción de no poder ser buscado. A pesar de los esfuerzos realizados, hay muchas cuestiones abiertas. Tal y como indica P. Fleischer (49) ¿Cómo gestionar el hecho de escribir un comentario/ imagen en el espacio de un usuario y que dicho comentario/ imagen sea copiado o re-distribuido? ¿Cómo gestionar el hecho de que un usuario escriba algo sobre otro? Además, con anterioridad a la eliminación de contenido es imprescindible contrastar este derecho con otros como el Derecho a la Libertad de Expresión o al Derecho de Acceso a la Información Pública, o incluso con las responsabilidades legales que se pueden derivar de un cierto contenido. Nótese la relación entre los distintos problemas puesto que preguntas como las indicadas se relacionan con el problema de la trazabilidad de usuarios y la inferencia de datos.

Dada la dificultad de gestionar los problemas que surgen a partir de las cuestiones planteadas, el "sentido común" es uno de los factores esenciales a considerar. En concreto, es imprescindible no sólo establecer leyes y derechos que contemplen estos problemas, sino también procedimientos detallados que especifiquen el modo de solventarlos. Asimismo, entornos colaborativos como son las RSs y la creciente necesidad de interoperabilidad (Sección III-E) provocan que los datos estén distribuidos, aumentando las dificultades para conseguir su completa eliminación. Por todos estos motivos, se ha de subrayar la necesidad de incluir procesos técnicos que permitan resolver el problema aquí planteado.

III-J. Manipulación indebida tras el acceso

Una cuestión que puede pasar desapercibida es el considerar qué ocurre una vez que los datos son entregados. Una vez que las políticas de control de acceso se verifican, en el caso de que la verificación sea satisfactoria y el dato solicitado es entregado ¿Qué ocurre después? ¿Se realizarán acciones, ej. descargas del dato, que violan la privacidad de los usuarios?

Éste es un tema de gran controversia en el que es indispensable indicar que las actividades realizadas fuera de las RSs, por ejemplo grabaciones o fotografías, están fuera del alcance. A este respecto, pero desde un punto de vista teórico, se plantean modelos de control de acceso, denominado modelos de control de uso (*usage control models*) (44). En concreto, este tipo de modelos controlan el acceso no sólo en la entrega de los datos, sino también a lo largo de todo su uso. Asociado con este problema, Gates plantea la necesidad de satisfacer el requisito *sticky policies*, el cual se basa en conseguir que las políticas de control de acceso estén vinculadas a los datos en todo momento y se mantenga el control sobre los mismos aun cuando son entregados (50).

Por otro lado, a nivel práctico y a pesar de las dificultades que este problema plantea, se distinguen dos grandes tipos de propuestas. La Criptografía Basada en Atributos (*Attribute Based Encryption, ABE*) es una de las posibles soluciones. Este tipo de criptografia utiliza atributos en la construcción de

claves o en la creación de las políticas de acceso, ayudando a controlar el acceso a los datos cada vez que son solicitados (37). Por otro lado, se hace uso de mecanismos que se despliegan en el lado del cliente para garantizar la verificación de las políticas en el momento de entrega de los datos. En concreto, A. C Squicciarini *et al.* proponen un mecanismo para limitar los usuarios que pueden acceder, subir o descargar un dato, siendo indispensable el establecimiento de un dispositivo de verificación de políticas (*enforcer*) en el lado del cliente (30). De forma similar, Kumari *et al.* presentan una aplicación, denominada SCUTA, que ha de instalarse en los navegadores. Las políticas están asociadas a los datos y, una vez que los datos alcanzan el navegador, las políticas se verifican (51).

En vista de las tendencias actuales, el principal problema radica en la necesidad de instalar o colocar algún tipo de mecanismo en el lado del cliente. Por ello, la criptografía basada en atributos parece ser una alternativa que ha de ser analizada en mayor profundidad puesto que, como en (52), es necesario el desarrollo de algoritmos que permitan establecer políticas más expresivas.

IV. Discusión

A la luz de los problemas identificados, dos cuestiones pueden destacarse. Por un lado, es conveniente determinar los problemas que, aún encontrándose algunas propuestas, no son el centro de las investigaciones actuales y presentan gran controversia. Por otro lado, atendiendo a las entidades participantes de las RSs, las cuales se pueden generalizar a datos y usuarios, es interesante estudiar cuáles de dichas entidades se ven afectadas por los problemas identificados, concluyéndose la necesidad de aumentar la protección de los datos y/ o de los usuarios.

IV-A. Problemas controvertidos

En particular, de todos los problemas estudiados, son el *Derecho al olvido* y la *Manipulación indebida tras el acceso* los problemas más controvertidos.

El *Derecho al olvido* suscita la necesidad de olvidar, replicar la mente humana. Sin embargo, este hecho resulta altamente contradictorio puesto que el mundo digital lleva intrínseca la característica de persistencia (53). De hecho, tal y como se comenta en la descripción de este problema, la cantidad de datos y la distribución de los mismos provocan que este "derecho" sea muy complejo de satisfacer, aún existiendo iniciativas legales en desarrollo, como el Reglamento Europeo, que van a obligar la adopción de medidas para tutelarlo (54).

Asimismo, la *Manipulación indebida tras el acceso* es otro de los problemas a los que es difícil enfrentarse. Es cierto que se pueden buscar soluciones que permitan paliar el problema, como la persistente verificación de políticas. No obstante, además de requerir que el usuario instale o sitúe un determinado mecanismo en su ordenador, siempre hay un periodo de tiempo que, por pequeño que sea (e.g. verificar la política), el dato puede estar fuera de control.

Como conclusión, es necesario señalar la complejidad y, a su vez, necesidad de proponer soluciones prácticas a estos dos problemas. Asimismo, hasta que se realicen avances y mejoras a este respecto, conviene subrayar la " obligación" de hacer un uso responsable de las RSs.

IV-B. Análisis de la privacidad

Aunque la privacidad repercute en los usuarios, es posible identificar qué entidades, de las involucradas en las RSs (usuarios y datos), son las directamente afectadas por cada problema. El análisis se presenta en la Tabla I.

A la vista de los resultados, el 50 % de los problemas afecta a los datos y otro 50 % a los usuarios. Por un lado, *Sybil nodes*, *Trazabilidad e inferencia de datos*, *Privacidad en la localización*, *Control de acceso simplificado* y *Anonimato de usuarios* son problemas que afectan directamente a los usuarios. Por otro lado, los problemas de *Co-propiedad*, *Interoperabilidad*, *Control de los datos almacenados*, *Derecho al olvido* y *Manipulación indebida tras el acceso*, afectan a los datos.

Por tanto, es posible subrayar que preservar la privacidad de los usuarios requiere ofrecer una protección global, en todas las dimensiones, es decir, prestando atención, en la misma medida, a los problemas que afectan directamente a los usuarios y a los que afectan directamente a los datos.

Cuadro I
Análisis de la privacidad

	Usuarios	Datos
Sybil nodes	√	
Co-propiedad		√
Trazabilidad e inferencia de datos	√	
Privacidad en la localización	√	
Interoperabilidad		√
Control de los datos almacenados		√
Control de acceso simplificado	√	
Anonimato de usuarios	√	
Derecho al olvido		√
Manipulación indebida tras el acceso		√

V. Conclusiones

En base a los recientes desarrollos y las numerosas investigaciones, se han identificado un total de diez problemas asociados con la privacidad de los usuarios en las RSs. Además, para cada uno de ellos se han propuesto futuras líneas de desarrollo. Por otro lado, se ha presentado una breve discusión de los problemas de mayor controversia y se ha analizado que para garantizar la privacidad de los usuarios se ha de prestar atención, al mismo nivel, a los problemas que afectan directamente a los datos y a los que afacten directamente a los usuarios.

Tras el estudio presentado, cabe destacar la necesidad de profundizar en las problemáticas y las posibles soluciones a cada uno de los problemas identificados. En especial, es importante trabajar en el estudio de los problemas de *Derecho al olvido* y *Manipulación indebida tras el acceso* puesto que, además de ser los más controvertidos, pocos has sido los autores que han realizado propuestas al respecto.

REFERENCIAS

[1] J. L. Becker and H. Chen, "Measuring privacy risk in online social networks," Ph.D. dissertation, University of California, Davis, 2009.

[2] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in *Privacy enhancing technologies*. Springer, 2006, pp. 36–58.

[3] R. Dey, Z. Jelveh, and K. Ross, "Facebook users have become much more private: A large-scale study," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*. IEEE, 2012, pp. 346–352.

[4] Espana, "Constitución española," Tech. Rep., 1978.

[5] R. Ajami, N. Ramadan, N. Mohamed, and J. Al-Jaroodi, "Security challenges and approaches in online social networks: A survey," *IJCSNS*, vol. 11, no. 8, p. 1, 2011.

[6] A. Ho, A. Maiga, and E. Aimeur, "Privacy protection issues in social networking sites," in *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*, 2009, pp. 271 –278.

[7] ENISA-members, "Position paper: Security issues and recommendations for online social networks," 2007.

[8] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," *Netwrk. Mag. of Global Internetwkg.*, vol. 24, no. 4, pp. 13–18, Jul. 2010.

[9] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, "Security issues in online social networks," *Internet Computing, IEEE*, vol. 15, no. 4, pp. 56–63, 2011.

[10] PrimeLife-Members, "Requirements and concepts for privacy- enhancing access control in social networks and collaborative workspaces," 2009.

[11] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, ser. SIGCOMM '06. ACM, 2006, pp. 267–278.

[12] W. Wei, F. Xu, and Q. Li, "Mobishare: Flexible privacy-preserving location sharing in mobile online social networks," in *INFOCOM, 2012 Proceedings IEEE*, 2012, pp. 2616 –2620.

[13] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based sybil defenses," in *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 4. ACM, 2010, pp. 363–374.

[14] B. Viswanath, A. Mislove, M. Cha, and K. P. Gummadi, "On the evolution of user interaction in facebook," in *Proceedings of the 2nd ACM workshop on Online social networks*, ser. WOSN '09. ACM, 2009, pp. 37–42.

[15] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in *Proceedings of the 18th international conference on World wide web*. ACM, 2009, pp. 521–530.

[16] A. C. Squicciarini, M. Shehab, and J. Wede, "Privacy policies for shared content in social network sites," *The VLDB Journal The International Journal on Very Large Data Bases*, vol. 19, no. 6, pp. 777–796, 2010.

[17] A. C. Squicciarini, H. Xu, and X. L. Zhang, "CoPE: Enabling collaborative privacy management in online social networks," *Journal of the American Society for Information Science and Technology*, vol. 62, no. 3, pp. 521–534, 2011.

[18] Y. Sun, C. Zhang, J. Pang, B. Alcade, and S. Mauw, "A trust-augmented voting scheme for collaborative privacy management," in *Proceedings of the 6th international conference on Security and trust management*, ser. STM'10. Springer-Verlag, 2011, pp. 132–146.

[19] V. Gligor, H. Khurana, R. Koleva, V. Bharadwaj, and J. Baras, "On the negotiation of access control policies," in *Security Protocols*. Springer, 2002, pp. 188–201.

[20] H. Hu, G. Ahn, and J. Jorgensen, "Multiparty access control for online social networks: model and mechanisms," 2012.

[21] K. Thomas, C. Grier, and D. Nicol, "unfriendly: Multi-party privacy risks in social networks," in *Privacy Enhancing Technologies*. Springer, 2010, pp. 236–252.

[22] H. R. Lipford, G. Hull, C. Latulipe, A. Besmer, and J. Watson, "Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites," in *Computational Science and Engineering, 2009. CSE'09. International Conference on*, vol. 4. IEEE, 2009, pp. 985–989.

[23] J. Lindamood, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "Inferring private information using social network data," in *Proceedings of the 18th international conference on World wide web*. ACM, 2009, pp. 1145–1146.

[24] E. Lalas, A. Papathanasiou, and C. Lambrinoudakis, "Privacy and traceability in social networking sites," in *Informatics (PCI), 2012 16th Panhellenic Conference on*. IEEE, 2012, pp. 127–132.

[25] H. Turner, T. Czauski, B. Dougherty, and J. White, "Dynamic tessellation to ensure k-anonymity," in *Computational Science and Engineering (CSE), 2012 IEEE 15th International Conference on*. IEEE, 2012, pp. 492–499.

[26] M. Burmester, "Localization privacy," *Cryptography and Security: From Theory to Applications*, pp. 425–441, 2012.

[27] M. Burmester_, "His late masters voice: Barking for location privacy," *Security Protocols XIX*, pp. 4–14, 2011.

[28] C.-m. A. Yeung, I. Liccardi, K. Lu, O. Seneviratne, and T. Berners-Lee, "Decentralization: The future of online social networking," in *W3C Workshop on the Future of Social Networking Position Papers*, vol. 2, 2009.

[29] L. González-Manzano, A. I. González-Tablas, J. M. de Fuentes, and A. Ribagorda, "U+F Social Network Protocol: Achieving interoperability and reusability between Web Based Social Networks," in *Trust, Security and Privacy in Computing and Communications (TrustCom),*

2012 IEEE 11th International Conference on, pp. 1387–1392.

[30] A. C. Squicciarini and S. Sundareswaran, "Web-traveler policies for images on social networks," *World wide web*, vol. 12, no. 4, pp. 461–484, 2009.

[31] J. Breslin, U. Bojars, A. Passant, S. Fernandez, and S. Decker, "Sioc: Content exchange and semantic interoperability between social networks," 2009.

[32] S.-W. Seong, J. Seo, M. Nasielski, D. Sengupta, S. Hangal, S. K. Teh, R. Chu, B. Dodson, and M. S. Lam, "Prpl: a decentralized social networking infrastructure," in *Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond*. ACM, 2010, p. 8.

[33] L. Aiello and G. Ruffo, "LotusNet: tunable privacy for distributed online social network services," *Computer Communications*, vol. 35, no. 1, pp. 75–88, 2012.

[34] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–9.

[35] R. Schlegel and D. Wong, "Private friends on a social networking site operated by an overly curious snp," *Network and System Security*, pp. 430–444, 2012.

[36] N. Kourtellis, J. Finnis, P. Anderson, J. Blackburn, C. Borcea, and A. Iamnitchi, "Prometheus: User-controlled p2p social data management for socially-aware applications," *Middleware 2010*, pp. 212–231, 2010.

[37] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: an online social network with user-defined privacy," in *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 4. ACM, 2009, pp. 135–146.

[38] K. Graffi, C. Gross, D. Stingl, D. Hartung, A. Kovacevic, and R. Steinmetz, "Lifesocial. kom: A secure and p2p-based solution for online social networks," in *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*. IEEE, 2011, pp. 554–558.

[39] A. Nourian and M. Maheswaran, "Towards privacy-preserving image template matching in the clouds," in *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, 2012, pp. 845 –850.

[40] C. Terwangne, "Internet privacy and the right to be forgotten / right to oblivion," *Revista de internet, derecho y política*, pp. 109 –121, 2012.

[41] F. Adu-Oppong, C. K. Gardiner, A. Kapadia, and P. P. Tsang, "Social circles: Tackling privacy in social networks," in *Symposium on Usable Privacy and Security (SOUPS)*, 2008.

[42] M. Vanetti, E. Binaghi, B. Carminati, M. Carullo, and E. Ferrari, "Content-based filtering in on-line social networks," in *Proceedings of the international ECML/PKDD conference on Privacy and security issues in data mining and machine learning*, ser. PSDML'10. Springer-Verlag, 2011, pp. 127–140.

[43] L. González−Manzano, A. I. González−Tablas, J. M. de Fuentes, and A. Ribagorda, *Security and Privacy Preserving in Social Networks*. Springer, exp.2013, ch. User-Managed Access Control in Web Based Social Networks.

[44] J. Park and R. Sandhu, "The UCON ABC usage control model," *ACM Transactions on Information and System Security (TISSEC)*, vol. 7, no. 1, pp. 128–174, 2004.

[45] P. Mittal, M. Wright, and N. Borisov, "Pisces: Anonymous communication using social networks," 2012.

[46] M. Bertier, D. Frey, R. Guerraoui, A.-M. Kermarrec, and V. Leroy, "The gossple anonymous social network," *Middleware 2010*, pp. 191–211, 2010.

[47] J. Camenisch and A. Lysyanskaya, "Dynamic accumulators and application to efficient revocation of anonymous credentials," *Advances in Cryptology, CRYPTO 2002*, pp. 101–120, 2002.

[48] J. Camenisch, "Information privacy?!" *Computer Networks*, 2012.

[49] P. Fleischer, "Foggy thinking about the Right to Oblivion," 2012.

[50] C. Gates, "Access control requirements for web 2.0 security and privacy," *IEEE Web*, vol. 2, no. 0, 2007.

[51] P. Kumari, A. Pretschner, J. Peschla, and J.-M. Kuhn, "Distributed data usage control for web applications: a social network implementation," in *Proceedings of the first ACM conference on Data and application security and privacy*. ACM, 2011, pp. 85–96.

[52] S. Braghin, V. Iovino, G. Persiano, and A. Trombetta, "Secure and policy-private resource sharing in an online social network," in *Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom)*. IEEE, 2011, pp. 872–875.

[53] W. Koehler, "Digital libraries and world wide web sites and page persistence," *Information Research*, vol. 4, no. 4, pp. 4–4, 1999.

[54] Parlamento-Europeo, "Reglamento del parlamento europeo y del consejo, 2012/0011 (COD)," http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF,\'ultimoaccesoAbril2013, 2012.