Análisis de herramientas para protección de datos personales

Enzo Notario[1], Bibiana Luz Clara[2], Beatriz P. de Gallo[3]
[1] enzo.notario@gmail.com, [2]luzbibianaclara@gmail.com, [3]bgallo@ucasal.edu.ar
IEsIIng, Facultad de Ingeniería, Universidad Católica de Salta

Abstract

La mayoría de proveedores de servicios en internet han sido desarrollados con un modelo de negocio basado en los datos de sus usuarios, sin pensar demasiado en su privacidad y haciendo un uso indebido de la confianza que estos le han otorgado. El modelo tradicional de aceptar los Términos y Condiciones de Uso ha caído en desuso ante los avances de la tecnología, y resultan difíciles y casi imposibles de entender para un usuario común. Las opciones que los usuarios tienen son dos: aceptar las condiciones o quedarse excluidos de los servicios. Además, en muchos casos, ni siquiera tienen la opción de elegir, ya que su privacidad se ve afectada por las decisiones de otras personas con las que establece ciertas relaciones. En este trabajo se discuten algunas de las herramientas orientadas a la protección de la privacidad de los datos, destacando la urgente necesidad de abordar este aspecto de la seguridad informática desde la perspectiva del propio usuario.

Palabras claves: *Herramientas para la protección de datos personales, seguridad informática, privacidad de los datos.*

1. Introducción

En la actualidad, cuando un usuario desea utilizar un servicio o un dispositivo electrónico, en la mayoría de los casos se requiere que éste inicie sesión de alguna manera en el sistema del fabricante. Por lo general, al iniciar sesión el usuario debe elegir entre continuar y aceptar los Términos y Condiciones (TC), o simplemente no aceptarlos y cancelar el proceso, quedándose excluido del uso total o parcial del servicio y/o dispositivo electrónico [1].

Los TC suelen incluir cláusulas que requieren el consentimiento de los usuarios para el intercambio de datos con fines comerciales. El típico *"He leído y acepto los términos y condiciones de uso"* es inadecuado, ya que estas cláusulas son muy largas y complicadas de entender para un usuario típico. Teniendo en cuenta que en términos técnicos y legales, consentir es autorizar, las personas muchas veces desconocen las consecuencias y simplemente optan por aceptar dichos TC, otorgándoles a distintas empresas información diversa y sumamente precisa. Además, muchos TC contemplan la posibilidad de ser actualizados sin previo aviso, lo que implica que los usuarios deben revisarlos constantemente para mantenerse informados.

El advenimiento del Internet de las Cosas (IoT) y los cincuenta billones de dispositivos IoT que se esperan para 2020, según *Juniper Research* [2], los cuales están provistos de distintos sensores capaces de recolectar datos de nuestros entorno, nos plantea el problema de la privacidad. Y es que, ante los avances de la tecnología, el modelo actual se ha quedado por detrás y es necesario un nuevo planteo que tenga en cuenta los tiempos modernos. Los usuarios desconocen muchas veces el destino que les será conferido a sus datos, además de no contar con la posibilidad de solicitar la eliminación de estos, aunque las leyes lo prevean.

Las Redes Sociales En Línea (OSN, del inglés *Online Social Networks*) son plataformas que agrupan a los usuarios de manera que pueden establecer amistades e interactuar unos con otros sobre sus actividades rutinarias [3]. Las OSN se han extendido de las redes convencionales debido a la evolución de Internet, de manera que estamos brindando gran parte de nuestros datos personales[1] a unas pocas OSN que no han sido diseñadas, desde su concepción, teniendo en cuenta la privacidad de sus usuarios.

Las OSN más populares, tales como *Facebook*, *Twitter* o *LinkedIn*, son servicios centralizados, que pertenecen y son gestionados por entidades comerciales individuales, de las cuales se sabe que aunque se presenten como un modelo de provisión de servicios gratuitos, se ven impulsados por el mercado dirigido y redirigido [4]. Estas dos estrategias de mercado se basan en recolectar y analizar la mayor cantidad de datos posibles de los posibles clientes, sus gustos, hábitos, sus patrones de consumos e incluso sus sentimientos y estados de ánimo [5].

Hemos entrado en la era de las Tecnologías que Invaden la Privacidad (PiTs, del inglés *Privacy-invading Techonologies*) y distintas investigaciones se han llevado a cabo tanto en los aspectos legales como en las

[1] Según el Artículo 4 de GDPR (http://www.privacy-regulation.eu/es/4.htm): Dato personal es toda información que pueda determinar, en particular mediante un identificador, la identidad de una persona física. Por ejemplo: nombre, número de identificación, datos de localización, estado físico, fisiológico, etc.

tecnologías que ayudan a proteger la privacidad (PETs, del inglés *Privacy-Enhancing Technologies*). Estas últimas son diseñadas desde el comienzo teniendo en cuenta la privacidad del usuario, lo que se conoce como Privacidad por Diseño (PbD, del inglés *Privacy by Design*).

Este trabajo estudia la problemática y las distintas alternativas de PETs y su aplicación en la actualidad. En la sección 2 se aborda el valor de los datos, la sección 3 describe algunas de las regulaciones actuales, en la sección 4 se detallan dos de las estrategias más usuales sobre protección de datos personales: protección por ocultamiento y protección por descentralización, la sección 5 detalla la herramienta MyData propuesta como una herramienta eficiente para la protección de privacidad de los datos de los usuarios; y por último, la sección 6 muestra las conclusiones arribadas de este estudio.

2. El valor de los datos

Pensemos por un momento en dos de los sensores que un teléfono inteligente tiene comúnmente: GPS integrado, capaz de determinar con suma precisión la ubicación en tiempo real de cada usuario, permitiendo conocer los lugares que visita y deducir sus vínculos con otros usuarios; Sensor de movimiento, capaz de deducir ciertos patrones de movimientos del usuario, produciendo datos que pueden ser usados para evaluar su salud, sus hábitos, etc. En el área automotriz, donde se estima que para el 2020 el 90% de los automóviles dispondrán de conectividad que permitirán una conducción más segura y eficiente, los datos generados por dicha conducción se vuelven sensibles ya que pueden revelar distintos aspectos del usuario, tales como sus hábitos y condición física [6].

Los problemas de privacidad y seguridad tienen consecuencias importantes para los usuarios y proveedores de servicios. Para los usuarios, las posibles consecuencias implican un intercambio inadecuado de información personal, es decir, fugas y distribución de detalles personales mediante la explotación activa, por ejemplo, *information linkage*[2]. Para los proveedores de servicios, las amenazas de privacidad y seguridad interrumpen su correcto funcionamiento y perjudican su reputación.

El término Privacidad ha sido definido por Westin en 1968 como el derecho de una persona a elegir qué datos personales desea que sean conocidos por los demás. Aunque esta definición sigue siendo válida, una adaptada al IoT [7] la define como la triple garantía para el sujeto de:

- Conocer los riesgos de privacidad impuestos por los dispositivos IoT y/o servicios que recogen los datos.
- Tener un control individual sobre la recopilación y el procesamiento de información personal por parte de los dispositivos IoT que lo rodean.
- La conciencia y el control del uso posterior y distribución de información personal por parte de las entidades a terceros.

La principales plataformas están controladas por proveedores individuales de forma centralizada y manejan una enorme cantidad de datos personales, lo que les permite realizar un análisis profundo e inferir información de sus usuarios tales como intereses personales, relaciones sociales, opiniones políticas, preferencias económicas, etc. Por ejemplo, *Facebook* ya controla datos privados de más la quinta parte de la población mundial, creciendo día a día con las recientes adquisiciones de *Instagram* y *WhatsApp* en 2012 y 2014, respectivamente. Con esto, *Facebook* obtiene fotos, números de teléfono y datos de mensajes para casi quinientos millones de usuarios y desde entonces trabaja para conectar estos datos con su servicio principal donde ya posee datos de intereses, localizaciones, rutinas, relaciones interpersonales, entre otros, de sus usuarios [8].

Particularmente con *Facebook*, en 2017 salió a la luz el escándalo que involucra a *Cambridge Analytica*, una compañía de estadísticas que pudo recolectar información precisa del día a día de ochenta y siete millones de personas, lo que les permitió inferir los hábitos y crear perfiles psicológicos detallados de los usuarios para ser usados durante las elecciones presidenciales de los Estados Unidos en el año 2016 [9]. Esto lo logró a través de la app para *Facebook*, *thisisyourdigitallife* una entre las más de veinticinco mil apps para *Facebook*[3] que con sólo haber sido utilizada por doscientos setenta mil usuarios, ha llegado a decenas de millones explotando la posibilidad de obtener datos de no sólo el usuario que utiliza la app, sino también de sus amigos.

Facebook alega que en ningún momento ha incumplido con los TC, y que ha sido *Cambridge Analytica* quien ha utilizado esos datos para otros fines.

De cualquier manera, está claro que ambas partes han sido perjudicadas, tanto los usuarios como *Facebook*, quien se estima que ha perdido unos sesenta billones de dólares inmediatamente después de haber ocurrido el escándalo [10].

[2] Se refiere a la vinculación de diferentes sistemas de modo que la combinación de las fuentes de datos revela información que previamente no fue revelada por las fuentes individuales [7].

[3] http://ai.sba-research.org/

3. Regulaciones actuales

Todo tratamiento de datos en Argentina debe cumplir con los recaudos que prevé la ley 25326 de Protección de Datos personales[4], que desde el año 2001 regula la materia, con sus modificaciones y reglamentación. A esto se suma que para la transferencia transfronteriza de datos se debe cumplir con los requisitos internacionales, que a partir del 25 de mayo de 2018 se han incrementado como consecuencia del nuevo Reglamento General de Protección de datos (RGPD), que la Unión Europea ha aprobado y puesto en funcionamiento, por lo cual las normativas de los distintos países que transfieren datos a la Unión Europea deberán ser adaptados a la nueva reglamentación, a efectos de mantener los mismos niveles de protección. Se centra principalmente en la privacidad de los datos personales, y los datos que se intercambian transfronteras, sobre todo luego del escándalo de *Facebook*, y *Cambridge Analytica*, por el supuesto uso indebido de los datos de los usuarios. El Reglamento incorpora la PbD y obliga a los sitios a pedir el consentimiento explícito de los usuarios para poder recabar datos personales, previendo aplicar serias multas y sanciones ante los incumplimientos por parte de las compañías.

En los Estados Unidos el sistema que se utiliza para proteger los datos denominado Escudo de privacidad, (*Privacy Shield*), es mucho más débil que la actual normativa europea, y se aplica al intercambio de datos entre USA y la UE.

Con la idea de examinar este sector y poder proponer cambios a la normativa nacional, se creó mediante Resolución 11/2017[5] en Argentina, el Observatorio de Big Data[6], en el ámbito de la Secretaria de Tecnologías de Información y Comunicación, con el objetivo de observar y analizar la evolución de esta tecnología y su incidencia en el proceso de innovación productiva, beneficios económicos y sociales para el público en general. Propone para ello la cooperación de organismos y entidades del ámbito público y privado, para el desarrollo del observatorio y la formulación de propuestas de modificaciones a la ley, con el aporte de todos los sectores involucrados.

Se trata de un desafío que traen las nuevas formas de procesar los grandes volúmenes de datos que no se condice con las formas tradicionales.

Big Data por el enorme volumen de datos y la alta velocidad con que los reúne permite predecir acontecimientos y mejorar la toma de decisiones, dotándolas de mayor eficacia.

Los datos son en nuestra era digital un activo clave, que permiten atraer nuevas oportunidades en los distintos rubros a los que se apliquen.

4. Protegiendo los datos personales

Las distintas investigaciones sobre PETs han tomado principalmente dos direcciones: La primera busca ocultar los datos personales a los proveedores de servicio. La segunda propone establecer un intermediario entre el usuario y los proveedores de servicios que centralice los datos y los distribuya en la medida que las configuraciones lo permitan. Estos intermediarios son construidos con PbD. Por lo tanto, buscan romper las barreras que los típicos TC de servicios imponen [11].

4.1 Protección de la privacidad por ocultamiento

El enfoque de estas investigaciones se basa en que la mayoría de productos y/o servicios pueden funcionar de manera correcta aunque se le brinde datos falsos. Estos datos falsos pueden obtenerse a partir de encriptar los verdaderos, o extraerse de algún diccionario de datos. Los datos encriptados podrían almacenarse en algún servicio de confianza del usuario, desde donde se gestione el acceso a los datos verdaderos por parte de otros usuarios. A continuación se dos implementaciones.

flyByNight [12]**:** Es una de las primeras aplicaciones para *Facebook* de este tipo que, aunque ha perdido vigencia, ha introducido el concepto de ocultamiento de datos: permite utilizar la red social sin enviar ninguna información sensible a los servidores de *Facebook* sin antes haber sido encriptados. Durante la configuración de la app, se genera una clave pública y una privada, más una contraseña que se utiliza para encriptar la clave privada, proceso del cual se obtiene la clave privada cifrada, que es almacenada en los servidores de *flyByNight*. Cuando un usuario instala la aplicación, se descarga un cliente *JavaScript*[7] que realiza las operaciones de encriptación. Este cliente conoce la lista de amigos del usuario que también utilizan *flyByNight* y sus claves públicas. Por ejemplo, para enviar un mensaje a sus amigos, el usuario ingresa el mensaje en la aplicación y selecciona a quien desea enviárselo. El cliente *JavaScript* encripta el contenido del mensaje con la clave pública del usuario receptor y etiqueta el mensaje encriptado con el identificador de *Facebook* del receptor. El mensaje encriptado es almacenado en los servidores de *flyByNight*. Cuando el receptor desea leer el mensaje, debe proveer su contraseña para obtener su clave privada (cuya versión cifrada se encuentra almacenada también

[4] http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm
[5] http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/275597/norma.htm
[6] www.bigdata.gob.ar
[7] https://developer.mozilla.org/es/docs/Web/JavaScript

en los servidores de *flyByNight*) y finalmente con la clave privada obtenida puede desencriptar el mensaje. Aunque esta aplicación opera bajo las regulaciones de *Facebook*, es posible que la carga de procesamiento que se genera en los servidores de *Facebook* debido a los mensajes encriptados llame la atención y termine siendo desactivada. En el peor de los casos, los usuarios perderán los mensajes enviados, pero al menos no podrán ser desencriptados por otros. Además, está claro que sólo funciona para *Facebook*.

Virtual Private Social Network **(VPSN)** [13]*:* Buscan proteger la privacidad del usuario sin agregar un tercer servicio, sino que utilizando los propios recursos de cada OSN para almacenar datos reales de otros usuarios, logrando así proteger la privacidad de cada usuario brindando datos falsos. *FaceVPSN* es la implementación para *Facebook* en forma de una extensión para el navegador web *Mozilla Firefox*. En *FaceVSPN* un usuario A debe cambiar su información de perfil con datos falsos en *Facebook* y envía los correctos a sus amigos en un formato XML[8]. Para que los amigos de A puedan conocer los datos verdaderos, deben tener también instalado *FaceVPSN* y utilizarlo para agregar el archivo XML que A les envió. Cuando un amigo de A visita el perfil de *Facebook* de A, éste provee los datos falsos. *FaceVPSN* captura los datos del perfil y busca los datos verdaderos en el archivo XML que ha sido guardado por cada amigo, y los reemplazando los falsos por los verdaderos.

Este enfoque no corre el riesgo de ser desactivado por las OSN, debido a que no dependen directamente de cada OSN, pero si requiere que cada usuario tenga instalada la extensión en su navegador web. Además cada usuario tiene que actualizar explícitamente los archivos XML que contienen los datos originales de sus amigos, lo cual lo hace poco usable, teniendo en cuenta que en promedio cada persona cuenta con más de dos cientos amigos, y el 15% con más de quinientos[9].

Este enfoque tiene la particularidad de depender, muchas veces, de las propias OSN. Además, dado el hecho de que las OSN operan con datos falsos (ya sea encriptado o reemplazados por otros) algunas funcionalidades pueden verse afectadas, como las búsquedas y recomendaciones basadas en el perfil de cada usuario. Además, los usuarios básicamente terminan transfiriendo su confianza de las OSN a terceros que proveen otro servicio más con TC incomprensibles. Por lo tanto, este enfoque se descarta [14].

4.2 Protección de la privacidad por la descentralización

Otra alternativa es descentralizar los proveedores de servicios y migrar a un tercer servicio diseñado con PbD. Las investigaciones en esta área proponen una arquitectura descentralizada (*peer-to-peer*[10]) para gestionar la información y así evitar los servicios centralizados que pueden obtener una visión global de la población.

Prometheus [15]: Es un sistema de gestión de datos personales *peer-to-peer* que no implementa las funcionalidades tradicionales de las OSN (creación de perfil, gestión de contactos, mensajería, etc.) sino que maneja la información de los usuarios desde varias fuentes de datos y expone una API para las aplicaciones sociales. Los datos de los usuarios son encriptados y almacenados en un grupo de pares de confianza seleccionados por el usuario teniendo en cuenta la disponibilidad del servicio. La inferencia de los datos está sujeta a la política de control de acceso definida por el usuario y protegida por los pares de confianza seleccionados.

MyData [16]: Es un sistema que pretende servir como base para brindarle al usuario la posibilidad de controlar su privacidad de manera fácil y centralizada, funcionando como intermediario entre los usuarios y los servicios provistos por las empresas, para quienes también aporta beneficios al centralizar los datos del usuario y proveer interfaces que permiten integrar servicios complementarios de terceros en sus servicios principales.

Esto lo logra descentralizando los proveedores de servicio y reuniendo los datos que los usuarios comparte con cada uno de ellos, brindándole la posibilidad de conocer de manera clara los fines para los que sus datos son utilizados, y retirar el consentimiento en cualquier momento, acoplándose a las distintas regulaciones de protección de datos personales. Esta herramienta se analizará con mayor detalle en la sección 5.

El gran desafío para este enfoque que busca descentralizar los proveedores de servicio es convencer a los usuarios de abandonar los servicios tradicionales y migrar a estos servicios descentralizados. Los servicios centralizados ya cuentan con una gran cantidad de usuarios establecidos y son accesibles desde cualquier parte. Tienen una infraestructura madura y mantienen una excelente usabilidad debido a que obtienen un gran beneficio a partir de los datos de los usuarios.

[8] https://developer.mozilla.org/es/docs/Introducci%C3%B3n_a_XML

[9] http://www.pewresearch.org/fact-tank/2014/02/03/what-people-like-dislike-about-facebook/

[10] Una red es de pares, o *peer-to-peer*, si los participantes comparten parte de sus recursos computacionales para proveer un servicio accesible por otros pares directamente, sin necesidad de entidades intermediarias (Schollmeier, 2002).

5. MyData

MyData es un modelo desarrollado en Finlandia que se refiere a 1) un nuevo enfoque, un cambio de paradigma en la gestión y procesamiento de datos personales que busca transformar el sistema centrado en la organización actual en un sistema centrado en humanos; 2) a datos personales como un recurso que el individuo puede acceder y controlar. Aquellos datos que el individuo no controle no se pueden llamar *MyData*.

Surge de una declaración escrita en 2017 por tres personas fuertemente envueltas en los Servicios de Gestión de Datos Personales: Antti Poikola, Daniel Kaplan y Tanel Mällo y actualmente es administrada por la *Open Knowledge Finland*[11] y *Aalto University*[12].

El concepto clave en la infraestructura propuesta es la *Cuenta MyData*. Para los individuos, una cuenta *MyData* es un centro único para la administración de datos personales. Con dicha cuenta, el individuo puede autorizar a los servicios a acceder y usar sus datos personales. La cuenta almacena información sobre cómo los datos personales del individuo están conectados a diferentes servicios y los permisos y consentimientos legales para usar los datos.

Esta PET se destaca por sobre el resto por brindarles beneficios todas las partes:

A los individuos: Proporciona una herramienta fácil de usar y comprender para gestionar sus datos personales, mecanismos transparentes que sólo muestra abiertamente como las organizaciones utilizan sus datos. Además gozan el beneficio de poder utilizar servicios innovadores y tener libertad de elección.

A los proveedores de servicios: Abre la oportunidad para nuevos tipos de negocios basados en los datos facilitando los aspectos técnicos y legales para el acceso de datos personales preexistentes cuando el individuo decide brindar su consentimiento. *MyData* está basado en estándares y desarrollado para soportar la interoperabilidad. Esto disminuye la barrera de entrada a nuevos negocios y permite un mercado más competitivo.

A la sociedad: *MyData* crea las estructuras, procesos y políticas necesarias para proteger los derechos de las personas y fomentar el uso de datos personales en el desarrollo de servicios innovadores.

En la arquitectura de *MyData*, los datos fluyen desde la fuente hacia los servicios y/o dispositivos que los utilizan. Aunque es importante entender que el flujo de consentimientos de permisos está separado del flujo de los datos. *MyData* no debe ser confundido con los sistemas de Almacenamiento de Datos Personales (PDS, del inglés *Personal Data Storage)*, que permiten almacenar los datos en un lugar seguro bajo control. La principal función de *MyData* es la gestión del consentimiento. Los datos no necesariamente deben ser transmitidos a través de los servidores donde se aloja la cuenta de *MyData*. La arquitectura estandarizada hace que las distintas cuentas sean interoperables y permite a las personas cambiar de operadores con facilidad. Para esto es necesaria una red en común que conecte los distintos nodos distribuidos.

[11] https://fi.okfn.org/
[12] http://www.aalto.fi/

6. Conclusiones

El principal obstáculo para que *MyData* se establezca es que va en contra de los intereses de las grandes empresas que controlan internet: *Google* y *Facebook*, ya que rompe sus modelos de negocio, los cuales se centran en la información que se deduce de los datos que los usuarios aportan día tras día y que comercializan con terceros. Además, aunque los componentes esenciales de *MyData* ya existen, aún requieren cierta maduración. Los elementos técnicos necesitan ser probados e integrados a los sistemas existentes.

Salvando los obstáculos, la infraestructura tecnológica que plantea *MyData* es similar a las que ya proveen empresas como *Google* y *Facebook*, que permiten a terceros desarrollar aplicaciones que consuman los datos que estas poseen sobre los usuarios, construidas sobre el *framework* de autorización *OAuth 2.0* [17], de uso común y fácil implementación. El siguiente paso será encontrar la manera de que los usuarios tomen importancia sobre este asunto y se preocupen en su privacidad.

Dado que *MyData* ha surgido en Finlandia, y que el reciente gobierno electo ha declarado que su plan de gobierno estratégico "*fortalecerá el derecho de los ciudadanos a monitorear y controlar el uso de sus datos personales, y al mismo tiempo garantizará el intercambio fluido de datos entre las autoridades públicas*", se da una combinación de prioridades que favorece a una adopción más rápida de los principios de *MyData*, que tiene la oportunidad de establecerse y marcarle los pasos a seguir al sector privado.

7. Agradecimentos

Los autores integran el equipo de trabajo del proyecto "Aplicación de Tecnologías Semánticas a la Forensia Digital: Estudio y Diseño de una Ontología aplicada a los Sistemas de Interconexión Digital de Objetos Cotidianos (IoT)" aprobado por el Consejo de Investigaciones de la UCASAL, a quien agradecen por hacer posible la presentación de este trabajo.

8. Bibliografía

[1] L. Belli, M. Schwartz, and L. Louzada, "Selling

your soul while negotiating the conditions: from notice and consent to data control by design," *Health Technol. (Berl).*, vol. 7, no. 4, pp. 453–467, 2017.

[2] Juniper Research, "IOT ~ THE INTERNET OF TRANSFORMATION 2018 Whitepaper," 2018.

[3] F. Li and T. C. Du, "The effectiveness of word of mouth in offline and online social networks," *Expert Syst. Appl.*, 2017.

[4] D. Meerman Scott, *The New Rules of Marketing and PR: How to Use Social Media, Blogs, News Releases, Online Video, and Viral Marketing to Reach Buyers Directly, 2nd Edition*. 2010.

[5] L. Bahri, B. Carminati, and E. Ferrari, "Decentralized privacy preserving services for Online Social Networks," *Online Soc. Networks Media*, 2018.

[6] Telefonica, "Connected Car Industry Report 2014," 2014.

[7] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: Threats and challenges," *Secur. Commun. Networks*, 2014.

[8] D. Koll, J. Li, and X. Fu, "The Good Left Undone: Advances and Challenges in Decentralizing Online Social Networks," *Computer Communications*. 2017.

[9] I. Symeonidis, G. Biczók, F. Shirazi, C. Pérez-Solà, J. Schroers, and B. Preneel, "Collateral damage of Facebook third-party applications: a comprehensive study," *Comput. Secur.*, 2018.

[10] A. Datoo, "Data in the post-GDPR world," *Comput. Fraud Secur.*, 2018.

[11] I. Kayes and A. Iamnitchi, "Privacy and security in online social networks: A survey," *Online Soc. Networks Media*, 2017.

[12] N. Borisov and M. M. Lucas, "FlyByNight: Mitigating the privacy risks of social networking Security and Privacy of Control Systems View project flyByNight: Mitigating the Privacy Risks of Social Networking," 2008.

[13] M. Conti, A. Hasani, and B. Crispo, "Virtual Private Social Networks and Facebook implementation," in *Proceedings of the first ACM conference on Data and application security and privacy - CODASPY '11*, 2013, p. 39.

[14] E. Balsa, L. Brandimarte, A. Acquisti, C. Diaz, and S. Gurses, "Spiny CACTOS: OSN Users Attitudes and Perceptions Towards Cryptographic Access Control Tools," in *Proceedings 2014 Workshop on Usable Security*, 2014.

[15] N. Kourtellis, J. Finnis, P. Anderson, J. Blackburn, C. Borcea, and A. Iamnitchi, "Prometheus: User-controlled P2P Social Data Management for Socially-aware Applications," in *Proceedings of the ACM/IFIP/USENIX 11th International Conference on Middleware*, 2010, pp. 212–231.

[16] A. Poikola, K. Kuikkaniemi, and H. Honko, "MyData," 2014.

[17] M. Jones and D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer Token Usage," 2012.

[18] R. Schollmeier, "A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications," 2002.