Privacidad y procesado automático de datos personales mediante aplicaciones y bots

Miguel Moreno Muñoz
Universidad de Granada
mm3@ugr.es

Privacy and Automatic Processing of Personal Data through Apps and Bots

Resumen: Los servicios prestados a través de redes digitales involucran a una compleja red de actores –no necesariamente humanos– que procesan información personal y explotan comercialmente sus ventajas. El desarrollo de aplicaciones y la introducción de bots y asistentes personales ligados a ecosistemas de servicios en la nube, cuyo desarrollo, supervisión y mejora depende con frecuencia de una sola empresa, añade complejidad adicional a este entramado de intermediarios y plantea riesgos específicos en materia de seguridad y privacidad. En este trabajo analizo las amenazas emergentes para la privacidad derivadas del empleo generalizado de aplicaciones y bots, en un contexto de demanda creciente de servicios gratuitos en la nube gestionados a través de dispositivos móviles.

Palabras clave: privacidad, seguridad, evaluación de riesgos, bots, aplicaciones, Internet de las cosas

Abstract: Services provided through digital networks involve a complex network of actors –not necessarily humans– in order to process personal information and be able of commercial exploitation of its advantages. The development of apps and the introduction of bots or personal assistants linked to ecosystems of services in the cloud –often depending on a single company– adds additional complexity to this network and raises specific risks for the security and privacy. In this paper I analyze the new threats to privacy associated with the widespread use of apps and bots, in a context of increasing demand for free services in the cloud through mobile devices.

Keywords: Privacy, security, risk evaluation, bots, apps, IoT

ISSN 1989-7022

Introducción

El incremento del número de usuarios conectados a Internet registra una evolución ascendente en el uso de dispositivos móviles (teléfonos o *tablets*). En 2012, el 23% de tales conexiones se realizaban desde *smartphones;* en octubre de 2016, las conexiones desde dispositivos móviles superaron por primera vez a las de usuarios conectados desde un ordenador, lo que supone multiplicar por 2,4 la cifra de 2012. En España, la conexión a Internet a través del móvil superaba en un diez por ciento la media global (85% a finales de 2016, seguida de Hong Kong, con un 79%). Esta misma tendencia se constata en China, Estados Unidos, Italia e India.[1]

India, en particular, destaca como el país donde más ha crecido el acceso a Internet a través de teléfonos móviles: duplica la tasa de países como Reino Unido (34,8%) y EE.UU. (37,2%), y es el país del G20 con mayor número de usuarios de móviles conectados a Internet.[2] Esta tendencia sugiere un cambio inminente de escenario tecnológico, donde el sistema Android de Google supera a Microsoft Windows como el sistema operativo con mayor base de

Received: 30/04/2017
Accepted: 05/05/2017

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

usuarios a escala mundial, si tomamos como referencia los datos combinados de uso total de Internet entre ordenadores de escritorio, portátiles, tabletas y dispositivos móviles.[3]

El incremento de las cuotas de participación que los nuevos actores están consolidando en la prestación de servicios globales a través de Internet evidencia el final de una era tecnológica, representada por el liderazgo mundial de Microsoft en el mercado de sistemas operativos desde la década de los ochenta. El rápido avance de Android –hace cinco años apenas canalizaba el 2,4% de los accesos a Internet– perfila la tendencia sociotécnica dominante y señala qué elementos de carácter estratégico –no detectados a tiempo por sus competidores– explican el incremento en la base mundial de usuarios de ciertos servicios y el abandono de otros.[4]

Si bien los usuarios de India, Emiratos Árabes o Corea del Sur se comportan como los del resto del mundo cuando se trata de realizar búsquedas (más del 90% usan el motor de Google), los porcentajes de acceso a ciertos servicios desde determinadas plataformas y dispositivos marcan la diferencia en términos de prospectiva sociotécnica. En este sentido adquiere relevancia el incremento de usuarios que acceden a Internet desde dispositivos móviles (4.917 millones de personas, o dos tercios de la población mundial) y generan más de la mitad del tráfico web, con un crecimiento del 30% respecto al año 2016. Este incremento va muy ligado a la demanda sostenida de uso de ciertas aplicaciones de mensajería (WhatsApp, SnapChat, WeChat, etc.) y acceso a redes sociales desde el móvil, que aumentó en un porcentaje similar con respecto al año anterior.[5]

La tendencia del mercado global a prestar servicios a través de dispositivos móviles conectados a Internet se estima que canalizará unos 134.000 millones de euros de gasto en publicidad en el año 2018, prácticamente el doble de lo calculado en 2016 y más que la suma total del destinado a periódicos, revistas, cine y publicidad al aire libre.[6]

La infraestructura para este mercado la aportan los sistemas de computación y almacenamiento de datos en la nube, accesibles a través de determinadas aplicaciones instaladas en dispositivos móviles ligeros y con recursos limitados, pero suficientes para interactuar con los sistemas (bots) que canalizan el tráfico de datos, reciben información del entorno físico y permiten gestionar el acceso a múltiples servicios.

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

Cada elemento integrado en esta infraestructura global de comunicaciones plantea riesgos específicos en términos de privacidad y seguridad (incluyendo a los usuarios humanos, con culturas de privacidad y niveles de alfabetización tecnológica muy diversos). Entre los incentivos para el desarrollo de la misma no debe olvidarse que figura el potencial para incrementar la vigilancia y control sobre consumidores, usuarios y ciudadanos por parte de actores estatales y privados (Weber and Studer 2016 Kshetri 2017; Mollah, Azad y Vasilakos 2017).

El objetivo de ese trabajo consiste en identificar los riesgos emergentes para la privacidad de usuarios de aplicaciones y dispositivos móviles conectados a servicios en la nube y redes sociales, en un contexto de servicios globales que registra un alto porcentaje de interacciones entre países que carecen de reciprocidad en el reconocimiento del derecho a la privacidad o reflejan culturas muy diferentes en sus políticas al respecto.

1. Apps

Las aplicaciones (abreviadas: *apps*) son programas diseñados para realizar funciones específicas que pueden ejecutarse en equipos de escritorio o en dispositivos móviles (multiplataforma). Muchas de ellas sólo requieren un navegador para ejecutarse (*web apps*), aunque no todas requieren conexión a internet. Suele utilizarse el término para describir cualquier software que no sea un programa completo, siendo versiones más simples destinadas al uso en dispositivos móviles, con pantallas de tamaño reducido e interacción táctil. Las *apps híbridas* tienen una interfaz de escritorio y acceso directo al hardware y a otros dispositivos conectados, pero pueden funcionar sin conexión.

Las aplicaciones móviles se obtienen de repositorios asociados con diversas plataformas, de las que pueden descargarse apps gratuitas o de pago. El acceso a las mismas se realiza normalmente a través de los dispositivos en las que pueden ser instaladas, o de sitios web donde los usuarios registrados las ponen en cola para su descarga la próxima vez que hagan uso del dispositivo móvil. Los repositorios de apps más conocidos son Google Play y Appstore (Amazon), para dispositivos móviles que funcionan con Android. Los usuarios de iPhone y iPad pueden obtenerlas a través de iTunes. Para equipos con sistema macOS, el lugar es Mac App Store; y para usuarios de Windows, la Windows Store.[7]

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

El empleo de apps constituye una tendencia imparable, y no sólo por el auge de sistemas como Android o iOS y el cambio de cultura asociado. Las restricciones para la informática móvil que conlleva el manejo de dispositivos móviles con pocos recursos están siendo superadas gracias a las tecnologías que permiten desplegar en la nube las tareas de almacenamiento de datos y de computación más exigentes, transfiriendo por vía inalámbrica el resultado al dispositivo móvil (Khan 2016).

La migración de información confidencial o datos personales a sistemas distribuidos de datos en la nube, con las medidas se seguridad habituales para optimizar el almacenamiento disponible y al mismo tiempo mantener tiempos de respuesta razonables en la prestación de servicios, plantea desafíos considerables en materia de seguridad y privacidad. Los mecanismos para autenticar usuarios móviles legítimos en el entorno de la nube se convierten, por razones obvias, en objetivo de ataque preferente.[8] Entre las contramedidas para identificar y neutralizar botnets figuran el recurso a sistemas de identificación biométricos (iris, huella dactilar, ultrasonidos) y la exigencia de respuestas que involucran elementos de razonamiento humano (CAPTCHA, p.ej.).[9]

Un entorno relativamente reciente para el consumo de apps, que plantea riesgos específicos, es el ligado al estándar HbbTV (*Abstract Hybrid Broadcast Broadband TV*), utilizado por la industria para proporcionar servicios combinados de televisión e Internet, mediante aparatos de TV conectados y decodificadores. Permite a los vendedores ofrecer aplicaciones directamente a los usuarios e introducir nuevos servicios de entretenimiento como *streaming* de vídeo bajo demanda,[10] juegos, redes sociales, etc. Se multiplican así los repositorios descentralizados con aplicaciones disponibles para que los usuarios descarguen y consuman contenidos en nuevos dispositivos conectados a Internet, lo que a su vez plantea nuevos problemas de confianza y seguridad. Los sistemas de gestión de la reputación y evaluación de recursos por parte de los usuarios exigen, además, que las tiendas de aplicaciones conozcan detalles de las aplicaciones instaladas y las recomendaciones proporcionadas por los usuarios, comprometiendo así su privacidad, a menos que se empleen medidas de cifrado y gestión de la identidad robustas (Tormo, Mármol y Pérez 2015: 226-229).

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

2. Bots

Empleado como aféresis de ro*bot*, su definición estándar (*un programa o agente informático autónomo, diseñado para imitar el comportamiento de usuarios humanos en tareas concretas y repetitivas*) no proporciona una idea muy precisa de la variedad de aplicaciones con las que pueden asociarse. Suelen estar programados para funcionar en redes, especialmente en Internet, e interactuar con otros sistemas o usuarios en tareas como la edición de textos, moderar conversaciones, responder a preguntas frecuentes –sobre un servicio, recurso informático o búsqueda de contenidos en la web, como hacen los bots conversacionales–, enviar correos electrónicos o dinamizar videojuegos, entre otras. Los más complejos se diseñan para tareas muy específicas, en las que compiten con usuarios humanos en el análisis de opciones y estrategias posibles (para vencer en videojuegos de rol, p.ej.).

Para aplicaciones complejas y servicios múltiples en la nube, las prestaciones de los bots pueden llegar a solaparse con funciones propias de sistemas expertos, utilizados para asistir a profesionales humanos en la toma de decisiones en contexto clínico, financiero, jurídico o asegurador, p.ej. (Truong, Phung, and Dustdar 2012). Los sistemas de monitorización que requieren la integración en tiempo real de información suministrada por sensores en diferentes localizaciones y devuelven información actualizada a petición de múltiples usuarios, procesada según ciertos filtros o algoritmos, pueden ser considerados otra variante en la tipología de bots, con funciones eventualmente críticas en la gestión del transporte (bots logísticos), el aprovechamiento de infraestructuras de alojamiento, planificación de rutas y mejoras de la eficiencia en el suministro de energía (Khajenasiri et al. 2017), entre otras.[11]

La simulación de escenarios de riesgo para la privacidad y la seguridad resulta de gran utilidad en todos los ecosistemas de servicios susceptibles de integrar bots en cualquier punto de la cadena de interacciones entre humanos y sistemas. Como ilustran Boshmaf et al. (2013), empleando un grupo de bots sociales programables coordinados fue posible desarrollar una campaña de infiltración a gran escala en un prototipo de sistema equiparable a Facebook. El principal resultado fue comprobar la facilidad con la que pueden ser explotados los comportamientos sociales bien conocidos de los usuarios de servicios como Facebook, puesto que la infiltración alcanzó una tasa de éxito del 80%. Dependiendo de los ajustes de privacidad en los perfiles de usuario, la infiltración realizada podía conllevar violaciones serias de la privacidad.

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 1-23

Aunque los incentivos económicos del mercado clandestino pudieran considerarse suficientes para hacer rentable una campaña de infiltración a gran escala, en ese momento no resultaban lo bastante atractivos como para hacer de esta actividad un negocio sostenible. Pero quedó demostrado el riesgo para los sistemas informáticos que utilizan o integran las plataformas de redes sociales en línea, y las limitaciones para arbitrar una defensa eficaz contra los bots sociales maliciosos derivadas de la automatización de la web, los niveles manejables de seguridad y el modo en que se establece la relación entre identidad física e identidad en la red. Si bien las medidas de seguridad implementadas parecían suficientes para alertar de una infiltración a gran escala ya desarrollada, no lo eran para prevenirla (Boshmaf et al. 2013: 557-558).

La incorporación de inteligencia artificial y *machine learning* permite diseñar bots capaces de aprender de sus interacciones con usuarios y mejorar la calidad de sus respuestas. La clave estará en la plataforma o base de datos de la que puedan extraer sus respuestas y en la precisión de las estadísticas sobre necesidades de los usuarios que puedan elaborar. Pero es relativamente fácil diseñar bots para extraer información personal y datos de interés industrial que comprometen la privacidad de individuos y empresas o que suponen una amenaza para la seguridad de servicios esenciales.

Diversas técnicas facilitan a los hackers infiltrarse en equipos personales de usuarios o empresas sin las medidas de seguridad apropiadas y usar tales equipos como bots para desplegar ataques cibernéticos, cometer fraude, robar información, enviar spam y propagar virus o troyanos. Por esta razón muchas compañías adoptan reglas muy estrictas para permitir el uso de bots, sobre todo en procesos donde resultaría fácil suplantar la identidad de los usuarios humanos (servicios de correo electrónico, redes sociales, sistemas para compartir archivos en la nube, etc.).[12]

Otras actuaciones maliciosas que suelen involucrar a bots atañen al fraude publicitario, el fraude con tarjetas de crédito y los ataques DDoS. Estos últimos son relativamente frecuentes y peligrosos, porque agotan los recursos de las aplicaciones haciéndoles generar contenido web dinámico, multiplicar las consultas a bases de datos o rehacer los índices de búsqueda, bloqueando su funcionamiento. Para evitar una detección temprana, los atacantes introducen código silencioso en los dispositivos diana y dividen la parte del malware que se ejecuta en cada bot, actualizando las *botnets* desde el servidor de comandos y control de vez en cuando. Los equipos zombis suelen ejecutar el código malicioso en segundo plano, y los usuarios objeto de

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

ataque tardan en darse cuenta de que su equipo está siendo utilizado como parte de una botnet gestionada por delincuentes.[13]

3. Internet de las cosas (IoT), datificación y Big data

El concepto "Internet de las cosas" (IoT), acuñado por Kevin Ashton,[14] se aplica a un sistema ciberfísico donde los objetos pueden conectarse a Internet a través de sensores ubicuos, dotándoles de funcionalidades decisivas en términos de disponibilidad, acceso, eficiencia en la distribución y contextualización. Se origina ligado al estándar de identificación automática (Auto-ID) para sensores de identificación por radio-frecuencia (RFID). Este sistema permite el almacenamiento y recuperación de datos remotos a través de dispositivos denominados etiquetas (pegatinas, tarjetas, transpondedores o tags RFID). La tecnología RFID se diseñó para transmitir la identidad de un objeto (algo parecido a un número de serie único) mediante ondas de radio.[15]

La conceptualización sugerida por Ashton no se limitaba estrictamente a los aspectos ingenieriles del estándar RFID. Le preocupaban las consecuencias del desajuste entre la actividad desarrollada en Internet por actores humanos, con una capacidad de tiempo, atención y precisión limitada, y la complejidad para contextualizar las características del mundo físico del que los seres humanos extraen datos relevantes para la toma de decisiones. Este desajuste tiene consecuencias decisivas en términos de eficiencia económica, distribución de recursos, dinamización de la vida social y estrategias de supervivencia o adaptación al entorno físico.

La digitalización y otros desarrollos técnicos que permiten avanzar en el proceso de convertir información previamente estática e inamovible en recursos dinámicos y transportables convergen hacia una Internet de los objetos: las ideas y la información seguirán siendo importantes, pero mejor contextualizadas y ajustadas a las características de un mundo físico sobre el que los objetos aportan datos de una precisión y escala mayor que la conseguida únicamente por actores humanos.

La información que circula entre ordenadores conectados procede, en su mayor parte, de la que han filtrado actores humanos según intereses específicos. Según Ashton, la recopilación de datos sin ayuda humana permitiría *rastrear y contar todo*,

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

y reducir el derroche, las pérdidas y los costes asociados a múltiples servicios. La tecnología RFID y otros sensores conectados a Internet permitirían a los sistemas informáticos *ver, oír y oler el mundo por sí mismos, en toda su aleatoria gloria, sin las limitaciones de los datos introducidos por el ser humano* (Ashton 2009).

La transición desde la web tradicional –centrada en ordenadores– a la Internet capaz de interconectar objetos cotidianos como relojes, rastreadores de actividad física (*wearables*), hornos, lavadoras, bicicletas, automóviles, plantas y animales o seres humanos en entornos cambiantes requiere nuevos sistemas de recolección, modelado y razonamiento sensibles al contexto (Perera et al. 2014). La fiabilidad de los datos aportados por sensores resulta un elemento crucial en este reto, así como el desarrollo de sistemas de computación sensibles al contexto (*context-aware computing*) para dar sentido a los datos de los sensores (Qin et al. 2016: 137-138).

El volumen del mercado potencial ligado a la IoT, sumado a otros elementos de la trayectoria tecnológica previa –herramientas de Big data, p.ej.– que convergen en la misma dirección, hacen previsible una expansión rápida y a escala global de los servicios asociados. Las estimaciones para 2016 aproximaban el número de objetos conectados a los 6.400 millones, con un aumento por año superior al 30%. Para 2020, Ericsson y Gartner amplían la cifra hasta los 50.000 millones, por la tendencia observada en el empleo de dispositivos y sistemas electrónicos en el hogar, la oficina o en los sistemas de transporte.[16]

La calidad, rapidez y fiabilidad de los sistemas de *datificación* (capacidad de producir datos que puedan ser leídos por un ordenador) constituye el elemento esencial en este proceso.[17] Algunos ejemplos de explotación combinada de las tecnologías de *Big data* e IoT: el ajuste de la oferta de contenidos mediante datificación del comportamiento de los usuarios de Netflix; el desarrollo de microcadenas de suministro, como efecto de la datificación de procesos comerciales; gestión más eficiente de los flujos de energía, ajustados a la demanda; modos optimizados de gestionar las ciudades, tras la implantación de sensores que aportan datos en tiempo real sobre transporte, calidad del aire, ruido, accidentes, etc.; adecuación de servicios ligados a la salud; incremento de medidas preventivas ante amenazas para la seguridad y la privacidad; estimaciones de riesgo más precisas como base para calcular las primas de seguros; gestión eficiente de la I+D y mejora de la base empírica y la metodología en los protocolos de investigación, entre otros (ver Ericsson 2014, nota 16).

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

Datificación, Internet de las cosas y Big data convergen sobre una base común de herramientas, tecnologías y procesos a gran escala que consolidan una tendencia a definir el modo en que las organizaciones o empresas tradicionales prestan sus servicios, entendidos en el nuevo contexto tecnológico como actividades dependientes de una infraestructura global de datos, de la que extraen conocimiento e información para desarrollar procesos críticos de su negocio, adoptar decisiones estratégicas y responder a la evolución de la competencia con un mejor control de los datos relevantes para su actividad (Mendelson y Mendelson 2017, 42-44).

Esta tendencia explica el carácter estratégico de los centros de datos como infraestructura básica para todo tipo de servicios en línea y su interés creciente como destino de posibles amenazas a la seguridad, a medida que miles de objetos se incorporan cada día como dispositivos permanentemente conectados (Zarpelão et al. 2017, 25-26, 32-34). Los datos son hoy el propulsor de crecimiento y transformación, como lo fue el petróleo en su momento. Y los flujos de datos configuran hoy nuevas infraestructuras, nuevos modelos de negocio y nuevas economías, con nuevos actores en posición de monopolio y políticas estatales diferenciadas según las ventajas de partida para beneficiarse de las reglas de mercado.[18]

La globalización digital ha incorporado a miles de empresas ubicadas en países en desarrollo a las redes de intercambio comercial que hasta hace relativamente poco dominaban unas pocas compañías transnacionales. Sistemas de comercio electrónico como Alibaba, Amazon, eBay, Flipkart y Rakuten canalizan aproximadamente un 12 por ciento del comercio mundial de bienes, y permiten a millones de pequeñas y medianas empresas en todo el mundo convertirse en exportadores mundiales, con capacidad para competir con grandes multinacionales.[19]

Aparte de los nuevas oportunidades de negocio asociadas al desarrollo de la IoT, conviene tener presente que una motivación específica para su implantación consiste en ampliar la capacidad de ciertos actores, privados o estatales, para vigilar y monitorizar las actividades de ciudadanos o usuarios de determinados servicios (Mendelson y Mendelson 2017: 42; Kshetri 2017: 55, 61, 63, 64; 2014; Weber y Studer 2016: 718). China, p.ej., parte de una posición privilegiada –en comparación con otros países industrializados– para liderar el desarrollo de la IoT por la gran base de usuarios que las empresas de tecnología chinas han conseguido capitalizar para desarrollar aplicaciones basadas en la IoT. Pero resulta obvio su interés en

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

monitorizar, controlar y censurar aspectos relevantes de la dinámica social y política dentro de su territorio, como hacen a diversa escala otros países involucrados en programas de vigilancia masiva.[20]

4. Bots sociales y riesgos de distorsión en el mercado laboral

Según Thomas L. Friedman, un análisis detenido de las convocatorias de empleo para puestos de trabajo "tradicionales" aporta pistas interesantes para comprender la transformación que a gran escala experimenta el mercado laboral, en un contexto de automatización creciente de tareas y consiguiente aumento de las exigencias de formación asociadas a los nichos tradicionales de empleo. En los puestos destinados a tareas administrativas y de secretaría, las exigencias han evolucionado hasta el punto de que cuatro quintas partes de quienes ahora ejercen esa profesión no cumplirían los requisitos para realizar un trabajo que, en los esencial, coincide con el que actualmente desempeñan.[21]

La diferencia está en que para el 65% de los puestos de trabajo ofertados se requiere una formación universitaria (licenciatura o grado), de la que carece el 81% de quienes desempeñan esos puestos en la actualidad. La distorsión obvia estriba en requerir capacidades que no se corresponden con las exigencias del puesto de trabajo a desempeñar, lo que aproxima a miles de candidatos a un escenario preocupante de subempleo o desempleo. Pero no cabe ignorar que las habilidades supuestamente requeridas se asocian ahora con la funcionalidad de aplicaciones de escritorio y servicios en gran medida automatizables o incorporados a las prestaciones de *bots* y de ciertas plataformas de trabajo en línea (Goh, Fung, and Depickere 2008).[22]

Exigir "capacidad de manejar código y programar en distintos lenguajes" o "habilidades desarrolladas para el manejo de datos" parece de entrada mucho más exigente que presuponer niveles medios de alfabetización digital, como correlato de las capacidades asociadas con tareas de gestión administrativa en las oficinas de hace una década. Pero el efecto distorsionador previsiblemente tendrá su reflejo en cómo el primer grupo termine asociado a las categorías salariales del segundo, más que a la inversa.

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

En términos de riesgos para la seguridad, es un hecho que muchas amenazas se hacen efectivas por las limitaciones de los actores humanos en su capacidad de estimar los riesgos y adoptar las estrategias preventivas adecuadas. Pero esta consideración no basta para justificar o incentivar, sin garantías muy estrictas de fiabilidad, la introducción de *bots* en sistemas de interacción en red como sustitutos de los primeros.

El riesgo de acceso indebido a información personal, de hipervigilancia, de distribución de *malware* y de difusión de noticias falsas se incrementa a medida que las redes sociales suman cada año a millones de usuarios activos y configuran una parte integral del ecosistema actual de servicios en Internet. En las manos equivocadas, unos pocos usuarios con las habilidades adecuadas pueden llegar a controlar *botnets* para perseguir sus fines, incluyendo los anteriormente señalados y otros –de previsibles consecuencias globales nefastas– como la alteración a su favor de la propaganda política (Nguyen, Rosoff y John 2016; Kshetri 2014: 1138, 1142) y del comercio algorítmico (Boshmaf, Muslukhov, Beznosov, and Ripeanu 2013).

5. Bots y riesgos de distorsión en los flujos de comunicación social

La difusión de noticias falsas propicia interpretaciones distorsionadas de la realidad y empobrece e intoxica la calidad del debate en asuntos de interés público. En la medida en que muchos medios han incorporado herramientas automáticas, gestionadas a través de bots sociales, para destacar y actualizar contenidos relevantes, se incrementa el riesgo de sesgos importantes en la toma de decisiones corporativas (por infravaloración o sobre-generalización de ciertos datos, p.ej.)[23] y se generan nuevas amenazas de desestabilización social o política cuando usuarios y máquinas amplifican el alcance de ciertos bulos al hacerlos circular en las principales redes sociales (Li et al. 2011; Ji et al. 2016).

Las estadísticas de ciberataques tienen con frecuencia su origen en un pequeño grupo de países, cuyos gobiernos amparan o indirectamente permiten a actores sin escrúpulos desarrollar acciones ilícitas. El objetivo suelen ser compañías estratégicas, dispuestas a pagar por mantener a salvo sus datos, en caso de sufrir brechas de seguridad.[24] Pero en las campañas electorales estadounidense y francesa de 2017 se ha comprobado que la interceptación de mensajes de adversarios políticos y

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

su difusión controlada puede distorsionar seriamente los procesos democráticos y promover escenarios con alto riesgo de confrontación social.[25]

La idea de una web desarrollada sobre un sistema de *confianza basada en el conocimiento* (Knowledge-Based Trust) no deja de ser, por el momento, un proyecto de investigación para reorientar la indexación de contenidos web en función de criterios endógenos (veracidad del contenido), en lugar de hacerlo por criterios exógenos (hiperenlaces a la página o sitio web).[26] Un problema aún por resolver es el relativo al sistema de filtrado encargado de alimentar la base de conocimientos que servirá de referencia y el tipo de recompensa para sitios de interés pero diseñados con fines ajenos a la difusión de hechos o noticias.

6. Políticas de privacidad

Los riesgos para la seguridad e integridad de los datos se incrementan cuando estos son gestionados mediante una explosión de aplicaciones móviles que conectan a los usuarios con una compleja oferta de servicios, recursos y datos en la nube.[27] Las políticas de privacidad que informan de tales riesgos y recomiendan prácticas seguras bajo criterios preventivos constituyen la primera línea de defensa de una empresa que gestiona un sitio web o presta servicios a través de una aplicación móvil.[28]

El rápido crecimiento de las oportunidades ligadas al Big data se ha producido sobre lo que muchos consideran un área gris a efectos reguladores, sin normas éticas y códigos de conducta bien establecidos que resulten eficaces para proteger adecuadamente a los consumidores del uso abusivo de su información personal por parte de los anunciantes. Muchas empresas carecen de guías de buenas prácticas y de políticas de privacidad adecuadas para impedir la revelación de información confidencial. Lamentablemente, los actores ilícitos desarrollan con frecuencia su actividad sobre los mismos bloques y series de datos que los usuarios legítimos, sin que su conducta molesta o peligrosa pueda tipificarse como delito por la debilidad o insuficiencia del marco regulador (Kshetri 2014: 1142).

La adopción de una política de privacidad no es suficiente, si no contribuye a promover prácticas entre los usuarios que minimicen el riesgo de conductas abusivas por parte de quienes aprovechan las zonas grises del marco regulador. Además, las políticas

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

de privacidad han de ser compatibles con objetivos que pueden colisionar entre sí, como son la sencillez de uso de ciertas aplicaciones, el acceso a información personal bajo ciertas condiciones y el potencial para compartirla con otros servicios y usuarios conectados, en un contexto de confianza y seguridad.[29] La dificultad para equilibrar de modo satisfactorio estos fines se incrementan a medida que cobra importancia el trabajo y la cooperación en redes para resolver problemas complejos e incrementar la eficiencia en tareas especializadas (Atzori, Iera, Morabito, and Nitti 2012).

Para actores con fines maliciosos, en ocasiones importa menos el acceso a las bases de datos con información personal (edad, sexo, ingresos, salud, etc.) que conocer los flujos de información asociados a ciertas actividades en tiempo real: compras, interacción social, archivos compartidos, servicios utilizados, datos proporcionados por sensores involucrados en tareas múltiples de monitorización y control (en el sector del transporte, la vigilancia, la atención médica, el ejercicio físico, etc.). De ahí que resulte importante concretar en las políticas de privacidad los datos personales mínimos requeridos para la prestación del servicio, diferenciados de los que exigirían una ampliación de los permisos iniciales para recibir prestaciones o servicios adicionales.[30]

La percepción de relevancia asociada con la protección de la privacidad (Hoofnagle and King 2008) ha evolucionado en función de las prestaciones de los dispositivos más utilizados y la oferta de servicios gratuitos, cuya rentabilidad se logra aplicando herramientas de Big data y procesado estadístico al flujo de datos que suministran los usuarios de determinados servicios. Algunos incidentes producidos por brechas en la seguridad de dispositivos y aplicaciones, incluso cuando tienen un alcance tan masivo como las prácticas de las agencias de inteligencia que desveló Edward Snowden en 2013 (Schuster, van den Berg, Larrucea, Slewe, et al. 2017), no parecen suficientes para contrarrestar la tendencia al uso de aplicaciones y servicios gratuitos con una cultura de la privacidad más sofisticada, como sería de esperar en usuarios tecnológicamente alfabetizados.[31]

Las políticas de privacidad deben concretar las garantías en caso de brechas en la seguridad y a qué datos acceden proveedores con requerimientos de privacidad diferentes, así como los procedimientos contemplados para ejercer el derecho a conocer la información personal de que dispone la empresa y su rectificación o eliminación. El equilibrio entre privacidad y usabilidad, decisivo en

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

las aplicaciones de comercio electrónico que rastrean la conducta de potenciales compradores incluso pagándoles por permitir este seguimiento (Parra-Arnau 2017; Li et al. 2011), sólo refuerza mecanismos de confianza en el servicio cuando aporta ventajas claras a los usuarios sin comprometer unas expectativas razonables de privacidad.[32]

7. Dificultades para concretar el alcance de *una expectativa razonable de privacidad*

Existe una falta de transparencia generalizada acerca de la información personal que las empresas de servicios que operan a través de Internet recopilan de sus clientes/usuarios y lo que hacen con ella.[33] En parte esto ocurre porque usuarios y empresas interaccionan en países con marcos legales y culturas de privacidad muy diversos. Pero la razón fundamental parece ser la disponibilidad de los usuarios a disfrutar de ciertos servicios y aplicaciones sin coste alguno asociado, aunque resulte obvio que el principal incentivo para sus desarrolladores sea la rentabilidad ligada al valor estratégico o de mercado que extraen de los datos y estadísticas de uso a gran escala (Truong, Phung, and Dustdar 2012).

La tendencia al uso de servicios en la nube mediante aplicaciones ligeras resulta imparable. A medida que se despliega la Internet de las cosas (IoT) y aumentan los recursos de computación en la nube, una base creciente de dispositivos siempre conectados permite la monitorización y optimización de equipos alojados en instalaciones geográficamente dispersas. En el entorno doméstico, aumenta la demanda de robots o asistentes para uso personal conectados a repositorios y servicios en Internet, con capacidad para procesar la información necesaria para reconocimiento de voz, objetos, navegación y realización de tareas en el mundo real (Pagallo 2013).

En consecuencia, resulta cada vez más difícil precisar en qué consiste "una expectativa razonable de privacidad", y las cuestiones legales o de gobernanza dependerán del contexto cultural de referencia y del tipo de aplicación o servicio del que se trate (ocio, salud, contactos, finanzas, gestión de pedidos, etc.). La difusión de aplicaciones y bots puede hacerse bajo políticas de gobernanza y privacidad múltiples, desde plataformas en la nube o en entornos distribuidos de

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

alojamiento, p.ej., y combinando el acceso a datos y dispositivos locales con el acceso a datos y características en la nube.

La dificultad para gestionar con garantías de seguridad y privacidad este tipo de servicios y la infraestructura asociada dependerá en gran medida de cómo los usuarios humanos usen, entrenen o administren sus bots en la nube, puesto que la interacción entre humanos y los sistemas de inteligencia artificial que hacen funcionar a los bots y mejorar su reglas de funcionamiento puede condicionar el tipo de información que consideren apropiado revelar, compartir o transferir en un determinado contexto. Una noción de "privacidad según diseño", que podría resultar aceptable entre bots centrados en servicios en la red y con potencial para recolectar datos incesantemente y de manera autónoma, podría no serlo para usuarios humanos con una cultura amplia de protección de datos personales (Pagallo 2013: 502).

Estos dispositivos de la IoT resultan idóneos –o al menos tanto como los ordenadores portátiles y los teléfonos inteligentes, en su mayoría con micrófono y cámara incorporados– como objetivos de ataque para quienes desarrollan programas de vigilancia (*spyware*). Su versatilidad tiene el inconveniente de que funcionan habitualmente conectados a redes y, por lo general, se sitúan muy cerca de sus usuarios, la mayoría de los cuales no suele adoptar medidas de precaución para evitar el acceso no autorizado al micrófono o a la cámara (Farley and Wang 2010).

8. Características de las mejores políticas de privacidad

Existen diversos recursos en línea para comparar las políticas de privacidad que aplican las principales empresas que desarrollan aplicaciones y prestan los servicios más demandados en Internet.[34] Entre las que mantienen una reputación favorable durante años destacan Abine, Mozilla y el buscador DuckDuckGo por su compromiso para evitar el rastreo de la actividad de sus usuarios sin necesidad de bloqueadores u otras herramientas externas.[35] Otra clasificación interesante podemos encontrarla en el Informe de la Electronic Frontier Foundation, *Who Has Your Back? 2016: Protecting Your Data From Government Requests*.[36] En su informe de 2013, p.ej., sólo unas pocas (Dropbox, Facebook, Foursquare, Google, LinkedIn, Loopt, Microsoft, Sonic.net y Twitter, entre las más conocidas)

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

exigían orden judicial para la retirada de contenidos, destacando las dos últimas por la robustez de su política integral de defensa de la privacidad de los usuarios frente a los gobiernos.[37]

Entre los elementos básicos de una política de privacidad destaca la *finalidad* (para qué se va a usar la información que el usuario decide compartir y para qué fines no); la *responsabilidad* (quiénes asumen la responsabilidad de proteger los derechos y privacidad de los usuarios); la *cantidad o elementos mínimos* de información personal requeridos para proveer el servicio –datos de registro, identidad, localización, etc.–; las *categorías de información no esencial*, para mejorar la funcionalidad o comodidad del servicio mediante el acceso a información técnica y sensores del dispositivo móvil utilizado, p.ej.; la *información que sólo se podrá compartir con autorización expresa*, si el hacerlo conllevara ventajas específicas o experiencias mejoradas (acceso a fotos en la galería, lista de contactos, micrófono y cámara del dispositivo, p.ej.).

Otros aspectos esenciales son los detalles relativos a qué información se transfiere a terceros y la no presunción de consentimiento otorgado por los usuarios, si este se produjo conforme a condiciones iniciales más estrictas.[38] En la práctica, esto conlleva mantener un registro actualizado de las condiciones asociadas a cada versión de la política de privacidad en una empresa, para facilitar en lo posible una comparación entre las nuevas exigencias y su versión original, en cada paso relevante de las autorizaciones que los usuarios otorgan para actualizar sus datos de registro en determinados servicios.

El contexto actual de hipervigilancia generalizada, promovida por actores estatales y privados dispuestos a utilizar todo tipo de estrategias para explotar según sus intereses la menor brecha de seguridad y tener acceso a información personal desde cualquier dispositivo conectado a Internet,[39] exige a las empresas precisar en sus políticas de privacidad si exigen siempre autorización judicial para dar acceso al contenido de las comunicaciones y si informan a los usuarios sobre las solicitudes de datos recibidas de entidades gubernamentales. La publicación de informes de transparencia y pautas de cumplimiento de la ley contribuye a reforzar la confianza de los usuarios en aquellas empresas que lo hacen, destacan en la lucha por el derecho a la privacidad de los usuarios en los tribunales y apoyan explícitamente iniciativas legislativas en esta dirección (Cardozo, Cohn, Higgins, Hofmann, et al. 2013).

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

9. Conclusión

Las garantías constitucionales que contribuyen a una protección efectiva de la privacidad no son efectivas sin mecanismos robustos de rendición de cuentas aplicables a quienes abusen o se lucren indebidamente con datos e información personal obtenidos de forma ilícita. El desequilibrio actual (difícilmente compatible con una *expectativa razonable de privacidad*) se explica en parte por el desajuste entre evolución tecnológica y las transformaciones de un marco regulador que, en lo fundamental, responde a criterios y escenarios de riesgo propios del contexto sociotécnico del siglo pasado.

Es preciso incorporar al debate social sobre las consecuencias de la convergencia de formatos en el soporte digital y la automatización de tareas los riesgos específicos asociados con la proliferación de dispositivos móviles de comunicación y de objetos conectados a Internet, en una dinámica expansiva de servicios en la nube que aprovecha de modo abusivo las zonas grises del marco regulador. Esta infraestructura ha consolidado modelos de negocio, pautas de consumo y estilos de ocio sustentados en un tráfico masivo de datos de carácter personal sin las debidas garantías de seguridad y privacidad, que favorece escenarios de abuso y vulnerabilidad para millones de usuarios.

La literatura reciente sobre los riesgos emergentes para la privacidad y la seguridad derivados de la progresiva implantación del Internet de las cosas, de la popularidad de determinadas aplicaciones y de la incorporación de bots o asistentes personales como mediadores habituales en la prestación de servicios a través de las redes digitales subrayan la importancia de familiarizar a los usuarios con las mejores políticas de privacidad. Su aplicación puede contribuir a promover buenas prácticas, reducir el riesgo de incidentes y ampliar la cultura de privacidad de los usuarios.

Referencias

Adewole, Kayode Sakariyah, Nor Badrul Anuar, Amirrudin Kamsin, Kasturi Dewi Varathan, and Syed Abdul Razak. Malicious accounts: Dark of the social networks. *Journal of Network and Computer Applications* 79, February 2017, 41–67.

ISSN 1989-7022

Ashton, Kevin. That "Internet of Things" Thing. *RFID Journal* 2009. Disponible en: http://www.rfidjournal.com/articles/view?4986.

Atzori, Luigi, Antonio Iera, Giacomo Morabito, and Michele Nitti. The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization. *Computer Networks* 56, November 2012, 3594–3608. Disponible en: http://linkinghub.elsevier.com/retrieve/pii/S1389128612002654.

Bal, Gökhan, Kai Rannenberg, and Jason I. Hong. Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns. *Computers & Security* 53, 2015, 187–202.

Boshmaf, Yazan, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. Design and analysis of a social botnet. *Computer Networks* 57, February 2013, 556–578.

Bottazzi, Giovanni, and Gianluigi Me. Chapter 17 - Responding to cyber crime and cyber terrorism—botnets an insidious threat A2 - Akhgar, Babak. Eds. Andrew Staniforth and Francesca B T - Cyber Crime and Cyber Terrorism Investigator's Handbook Bosco, 231–257, Syngress, 2014 .

Broad, James, and Andrew Bindner. Chapter 10 - Maintaining Access BT - Hacking with Kali. 167–180, [Boston]: Syngress, 2014.

Cardozo, Nate, Cindy Cohn, Parker Higgins, Marcia Hofmann, and Rainey Reitman. *2013 - Who Has Your Back: Which Companies Help Protect Your Data from the Government? The Electronic Frontier Foundation's Third Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data*. 2013 Disponible en: https://www.eff.org/sites/default/files/who-has-your-back-2013-report-20130513.pdf.

Elliott, Claire. Botnets: To what extent are they a threat to information security? *Information Security Technical Report* 15, August 2010, 79–103.

Farina, Paolo, Enrico Cambiaso, Gianluca Papaleo, and Maurizio Aiello. Are mobile botnets a possible threat? The case of SlowBot Net. *Computers & Security* 58, May 2016, 268–283.

Farley, Ryan, and Xinyuan Wang. Roving bugnet: Distributed surveillance threat and mitigation. *Computers & Security* 29, July 2010, 592–602.

Goh, Ong Sing, Chun Che Fung, and Arnold Depickere. Domain knowledge query conversation bots in instant messaging (IM). *Knowledge-Based Systems* 21, October 2008, 681–691.

Hoofnagle, Chris Jay, and Jennifer King. What Californians Understand about Privacy Online. *SSRN Electronic Journal* 2008. Disponible en: http://www.ssrn.com/abstract=1262130.

Iqbal, Salman et al. On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *Journal of Network and Computer Applications* 74, October 2016, 98–120.

Ji, Yuede, Yukun He, Xinyang Jiang, Jian Cao, and Qiang Li. Combating the evasion mechanisms of social bots. *Computers & Security* 58, May 2016, 230–249.

Khajenasiri, Iman, Abouzar Estebsari, Marian Verhelst, and Georges Gielen. A Review on Internet of Things Solutions for Intelligent Energy Control in Buildings for Smart City Applications. *Energy Procedia* 111, March 2017, 770–779. Disponible en: http://linkinghub.elsevier.com/retrieve/pii/S1876610217302692.

Khan, Minhaj Ahmad. A survey of security issues for cloud computing. *Journal of Network and Computer Applications* 71, August 2016, 11–29.

Kshetri, Nir. Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy* 38, December 2014, 1134–1145. Disponible en: http://linkinghub.elsevier.com/retrieve/pii/S0308596114001542.

Kshetri, Nir. The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply. *Telecommunications Policy* 41, 2017, 49–67.

Li, Min, Xiaoxun Sun, Hua Wang, Yanchun Zhang, and Ji Zhang. Privacy-aware access control with trust management in web service. *World Wide Web* 14, 2011, 407–430.

Mansfield-Devine, Steve. Monitoring communications: the false positive problem. *Computer Fraud & Security* 2013, September 2013, 5–11.

Mansfield-Devine, Steve. Ransomware: taking businesses hostage. *Network Security* 2016, October 2016, 8–17. Disponible en: http://linkinghub.elsevier.com/retrieve/pii/S1353485816300964.

Mendelson, D., and D. Mendelson. Legal protections for personal health information in the age of Big Data – a proposal for regulatory framework. *Ethics, Medicine and Public Health* 3, 2017, 37–55.

Mollah, Muhammad Baqer, Md. Abul Kalam Azad, and Athanasios Vasilakos. Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications* 84, 2017, 38–54.

Nguyen, Kenneth D., Heather Rosoff, and Richard S. John. The effects of attacker identity and individual user characteristics on the value of information privacy. *Computers in Human Behavior* 55, 2016, 372–383.

Pagallo, Ugo. Robots in the cloud with privacy: A new threat to data protection? *Computer Law & Security Review* 29, October 2013, 501–508.

Parra-Arnau, Javier. Pay-per-tracking: A collaborative masking model for web browsing. *Information Sciences* 385–386, April 2017, 96–124.

Perera, Charith, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. Context Aware Computing for The Internet of Things: A Survey. *IEEE Communications Surveys & Tutorials* 16, 2014, 414–454. Disponible en: http://ieeexplore.ieee.org/document/6512846.

Qin, Yongrui et al. When things matter: A survey on data-centric internet of things. *Journal of Network and Computer Applications* 64, April 2016, 137–153. Disponible en: http://linkinghub.elsevier.com/retrieve/pii/S1084804516000606.

Rabotka, Vladimir, and Mohammad Mannan. An evaluation of recent secure deduplication proposals. *Journal of Information Security and Applications* 27–28, April 2016, 3–18.

Schuster, Stefan, Melle van den Berg, Xabier Larrucea, Ton Slewe, and Peter Ide-Kostic. Mass surveillance and technological policy options: Improving security of private communications. *Computer Standards & Interfaces* 50, 2017, 76–82.

Seewald, Alexander K, and Wilfried N Gansterer. On the detection and identification of botnets. *Computers & Security* 29, February 2010, 45–58.

Tormo, Ginés Dólera, Félix Gómez Mármol, and Gregorio Martínez Pérez. Towards privacy-preserving reputation management for hybrid broadcast broadband applications. *Computers & Security* 49, March 2015, 220–238.

Truong, Hong-Linh, Phu H Phung, and Schahram Dustdar. Governing Bot-as-a-Service in Sustainability Platforms – Issues and Approaches. *Procedia Computer Science* 10, 2012, 561–568.

ISSN 1989-7022

ISSN 1989-7022

Weber, Rolf H, and Evelyne Studer. Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review* 32, October 2016, 715–728.

Zarpelão, Bruno Bogaz, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications* 84, April 2017, 25–37. Disponible en: http://linkinghub.elsevier.com/retrieve/pii/S1084804517300802.

Zhao, David et al. Botnet detection based on traffic behavior analysis and flow intervals. *Computers & Security* 39, Part A, November 2013, 2–16.

Notas

1. Cfr. https://www.zenithmedia.com/mobile-forecasts-75-internet-use-will-mobile-2017.

2. Cfr. http://gs.statcounter.com/press/india-amongst-world-leaders-in-use-of-mobile-to-surf-the-internet.

3. Según StatCounter, compañía de analítica web, en marzo de 2017 Android superó con un 37,93% (ligeramente por delante del sistema Windows, con un 37,91%), la cuota en el mercado mundial de uso de Internet. Cfr. http://gs.statcounter.com/press/android-overtakes-windows-for-first-time.

4. Aunque la plataforma Windows continúa siendo mayoritaria en términos globales (38,6%), seguida de Android (37,4%) e iOS (13%), lo relevante es comprobar cómo evolucionan estos porcentajes en los 2-3 últimos años y qué lugar ocupan en aquellos países que mejor reflejan la tendencia global. En India, Android tienen una penetración del 62%, seguido por Windows (19,4%). Los usuarios que acceden a Internet a través de ordenador de mesa o portátil (45% del total) suponen en 2017 un 20% menos que en 2015. Y el uso de tabletas pierde peso, pasando de un 10% previo a sólo un 5% en 2017. Cfr. https://marketing4ecommerce.net/usuarios-de-internet-mundo-2017; http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html.

5. Cfr. Informe "We Are Social 2017" (págs. 5, 6, 46 y 50), disponible en: http://www.slideshare.net/wearesocialsg/digital-in-2017-global-overview?ref=https://thenextweb.com/insights/2017/01/24/digital-trends-2017-report-internet/; https://dazeinfo.com/2016/06/13/number-internet-users-worldwide-2016-2020; http://www.internetworldstats.com/stats.htm.

6. Cfr. http://www.reuters.com/article/us-internet-mobilephone-idUSKCN12S29L.

7. Cfr. https://www.lifewire.com/what-are-apps-1616114; https://play.google.com/store?hl=es; https://itunes.apple.com; https://www.apple.com/ca/osx/apps/app-store; https://www.microsoft.com/es-es/store/apps/windows.

8. Cfr. http://www.grupocmc.es/cmc-se-une-nozomi-lanzar-espana-una-tecnologia-reduce-tiempo-deteccion-ciberataques;
https://www.akamai.com/us/en/about/news/press/2016-press/akamai-revolutionizes-bot-management.jsp; https://www.zenedge.com/malicious-bot-bad-bot-detection-mitigation.

9. Cfr. https://www.merca20.com/todo-lo-que-necesitas-saber-sobre-los-bots-en-redes-sociales; https://www.akamai.com/us/en/about/news/press/2016-press/akamai-revolutionizes-bot-management.jsp.

10. La retransmisión de vídeo por *streaming* permite la visualización y audición de un archivo mientras se está descargando. El consumo de contenidos de vídeo bajo demanda ocupa ya más tiempo que

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

el consumo de TV. Cfr. Deloitte, *2016 US Global mobile consumer survey*. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-global-mobile-consumer-survey-2016-executive-summary.pdf; y https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-2017-media-and-entertainment-industry-outlook.pdf.

11. Cfr. https://wiki.factorio.com/Logistic_network; http://www.mhi.org/media/members/49084/130108044949168372.pdf; https://www.hosteltur.com/120165_machine-learning-bots-small-data-al-servicio-experiencia-hotelera.html; https://www.hosteltur.com/comunidad/005170_bots-y-turismo-una-oportunidad-historica.html;

12. Cfr. Rabotka y Mannan 2016; Weber y Studer 2016; Mollah, Azad y Vasilakos 2017; Adewole et al. 2017; Iqbal et al. 2016.

13. Una *botnet* es una red de computadoras infectadas con software malicioso (o *malware*), que permite a un atacante controlar ciertos dispositivos o equipos, por lo general sin el conocimiento del propietario. Las botnets se utilizan para cometer una extensa variedad de delitos cibernéticos. Cfr. Mansfield-Devine 2016 y 2013; Broad y Bindner 2014; Elliott 2010;Zhao et al. 2013; Bottazzi y Me 2014; Farina et al. 2016; Seewald y Gansterer 2010.

14. Kevin Ashton elaboró un sistema para conectar objetos cotidianos del mundo físico a Internet a través de sensores ubicuos (el estándar mundial para RFID y otros sensores). Su idea de una "Internet de los objetos" comenzó a circular en 1999, y fue consolidándose a medida que se producía la convergencia hacia el formato digital y surgían nuevas oportunidades para la industria y el comercio ligadas a la posibilidad de integrar a cada objeto como una parte de Internet. Cfr. Ashton, K. (2009), That 'Internet of Things' Thing. Disponible en: http://www.rfidjournal.com/articles/view?4986.

15. Una vez adherida o incorporada la etiqueta RFID a un producto, puede recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren. Entre otras ventajas, el uso de radiofrecuencia no requiere visión directa entre emisor y receptor (a diferencia, p.ej., de la identificación de objetos mediante códigos de barras), permite almacenar más información que otros sistemas alternativos y pueden ser reprogramados. Cfr. https://es.wikipedia.org/wiki/RFID.

16. Cfr. Ericsson (2014), *The Impact of Datafication on Strategic Landscapes*. Disponible en: http://www.ericsson.com/res/docs/2014/the-impact-of-datafication-on-strategic-landscapes.pdf; Gartner (2015), Top Strategic Predictions for 2016 and Beyond: The Future Is a Digital Thing. Disponible en: https://www.gartner.com/doc/3142020/top-strategic-predictions-future-digital.

17. Cfr. http://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world.

18. Cfr. *The Economist*, May 06, 2017: 9. Disponible en: http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource; N. Rivera, 20/06/2015, https://hipertextual.com/2015/06/internet-of-things.

19. Cfr. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

20. Cfr. K. Voigt (2012), "China looks to lead the Internet of Things". Disponible en: http://www.cnn.com/2012/11/28/business/china-internet-of-things; N. Kobie, "What is the internet of things?", 6/05/2015. Disponible en: https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google; D. Sarabia, "La NSA almacenó más de 150 millones de llamadas en 2016 pese a los cambios en la ley", 03/05/2017. Disponible en: http://www.eldiario.es/cultura/tecnologia/privacidad/NSA-almaceno-millones-llamadas-cambios_0_639736184.html.

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 1-23

21. Cfr. T. L. Friedman, "How to Beat the Bots". *The New York Times*, 10/06/2015. Disponible en: https://www.nytimes.com/2015/06/10/opinion/thomas-friedman-how-to-beat-the-bots.html?_r=0

22. El trabajo de Goh et al. muestra el potencial de ciertos *bots* conversacionales en un sistema de mensajería instantánea. Sobre un sistema de inteligencia artificial diseñado para procesar lenguaje natural, el resultado tras miles de interacciones muestra un porcentaje notablemente alto de aciertos en consultas relativas a un dominio específico de conocimiento, y bajo nivel de errores o respuestas no pertinentes. Es interesante comprobar la amplitud y heterogeneidad de las fuentes documentales utilizadas, así como la carga de trabajo y nivel de especialización que se requeriría para obtener un resultado equivalente con operadores humanos (Goh, Fung y Depickere 2008: 685).

23. Cfr. T. Chatfield (5/05/2013), "La verdad de las mentiras en internet", disponible en: http://www.bbc.com/mundo/movil/noticias/2013/05/130503_internet_web_mentiras_finde.shtml; y M. McGee (3/03/2015), "Google Researchers Introduce System To Rank Web Pages On Facts, Not Links", disponible en: http://searchengineland.com/google-researchers-introduce-system-rank-web-pages-facts-not-links-215835.

24. Cfr. http://www.bbc.com/mundo/noticias-39903218; https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html; https://www.certsi.es/alerta-temprana/avisos-seguridad/oleada-ransomware-afecta-multitud-equipos; https://www.incibe.es/protege-tu-empresa/avisos-seguridad/otra-oleada-ransomware-suplantando-correos.

25. Cfr. http://www.europapress.es/internacional/noticia-equipo-macron-insinua-supuesta-injerencia-rusa-elecciones-20170213152748.html; http://internacional.elpais.com/internacional/2017/04/25/actualidad/1493134783_069673.html.

26. Cfr. X. Luna Dong et al. (2015), "Knowledge-Based Trust: Estimating the Trustworthiness of Web Sources", Proceedings of the VLDB Endowment. Disponible en: https://arxiv.org/pdf/1502.03519v1.pdf.

27. Cfr. http://www.abc.es/tecnologia/moviles/20140324/abci-alerta-seguridad-android-201403241353.html; http://blog.elhacker.net/2017/04/apps-fraudulentas-en-google-play-android.html; https://www.cnet.com/how-to/how-to-spot-fake-ios-and-android-apps; http://www.nytimes.com/2016/11/07/technology/more-iphone-fake-retail-apps-before-holidays.html.

28. Cfr. http://searchdatacenter.techtarget.com/es/cronica/Mas-alla-de-las-politicas-de-privacidad-Privacidad-practica-para-sitios-web-y-apps-moviles.

29. Cfr. http://www.pewinternet.org/2014/11/12/public-privacy-perceptions.

30. Este criterio se mantiene con claridad en la política de privacidad Spotify, p.ej. Cfr. https://www.spotify.com/es/legal/privacy-policy.

31. Cfr. K. Drum (2013), "Privacy is dead. Long live transparency!". Disponible en: http://www.motherjones.com/politics/2013/10/future-of-privacy-nsa-snowden; y M. Madden (2014), "Public perceptions of privacy and security in the post-snowden era". Pew Research Center's Internet & American Life Project. Disponible en: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions.

32. Cfr. W. Enck et al. (2010), citado por Bal, Rannenberg y Hong 2015: 189.

33. Cfr. https://www.forbes.com/sites/adamtanner/2013/09/11/here-are-some-of-americas-most-privacy-friendly-companies/#549d58b75d15.

34. Cfr. http://data-informed.com/7-best-privacy-practices-for-companies-managing-customer-data; http://readwrite.com/2009/07/23/15-top-privacy-policies-analyz; http://www.wnd.com/2014/05/best-and-worst-companies-for-internet-privacy; https://www.acrolinx.com/blog/content-matters-the-companies-with-the-best-and-worst-privacy-policies-and-why-you-should-care; http://time.com/3986016/google-facebook-twitter-privacy-policies.

35. Destaca la posición que ocupan, por este orden, Airbnb, Flipkey, Getaround, Instacart, Lyft, Postmates, Taskrabbit, Turo y Uber, entre otras. Cfr. https://www.forbes.com/sites/adamtanner/2013/09/11/here-are-some-of-americas-most-privacy-friendly-companies/#549d58b75d15.

36. Disponible en: https://www.eff.org/who-has-your-back-2016.

37. Cfr. https://www.eff.org/sites/default/files/who-has-your-back-2013-report-20130513.pdf.

38. Cfr. http://searchdatacenter.techtarget.com/es/cronica/Mas-alla-de-las-politicas-de-privacidad-Privacidad-practica-para-sitios-web-y-apps-moviles.

39. Cfr. http://www.washingtontimes.com/news/2017/apr/12/russia-gives-hackers-immunity-exchange-stolen-data.

ISSN 1989-7022 **DILEMATA**, *año 9 (2017), nº 24, 1-23*