Gazeta de Antropología

ISSN 0214-7564
En Internet: ISSN 2340-2792

Gazeta de Antropología, 2018, 34 (2), artículo 08 · Versión HTML

Recibido 4 diciembre 2018 | Aceptado 18 diciembre 2018 | Publicado 2018-12

Mediación tecnológica de la interacción social y riesgos de su instrumentalización. El caso de la plataforma Facebook

Technological mediation of social interaction and the risks of its instrumentalization. The case of the Facebook platform

Miguel Moreno Muñoz
Profesor Contratado Doctor (acreditado para TU). Departamento de Filosofía II, Universidad de Granada. España
mm3@ugr.es

FILOSOFÍA Y ANTROPOLOGÍA. HOMENAJE A PEDRO GÓMEZ
MONOGRÁFICO COORDINADO POR MIGUEL MORENO (Universidad de Granada)

RESUMEN
Las redes sociales en línea (OSN) se han constituido en mediadores ineludibles de las dinámicas de interacción social. Plataformas como Facebook han crecido integrando servicios que las convierten en ecosistemas de ocio, consumo y negocio en la práctica imprescindibles para un tercio de la población humana. Partiendo de un estudio contextualizado de las brechas de seguridad e incidentes conocidos entre 2014 y 2018, mi trabajo analiza los riesgos de una instrumentalización de Facebook a gran escala por actores privados y estatales bajo una triple hipótesis: (1) se agravaron o materializaron en gran parte como resultado del diseño y características implementadas en la plataforma Facebook; (2) dichas características iban estrechamente ligadas a su núcleo de negocio, una vez definido y explotado con éxito; y (3) la política de adquisiciones de empresas o servicios de terceros —Instagram y WhatsApp, entre otros— reforzó su orientación como servicio global bajo criterios de rentabilidad, en detrimento de las garantías para la privacidad de los usuarios y la fiabilidad de la plataforma. Entre otros resultados, se identifican aspectos ligados al diseño/gestión de las OSN que pueden condicionar negativamente la calidad del debate público a diversas escalas y demandarían ajustes en el marco regulador.

ABSTRACT
Online Social Networks (OSNs) have become inescapable mediators of social interaction dynamics. Platforms such as Facebook have grown integrating services that turn them into ecosystems of leisure, consumption and business, in practice essential for a third of the human population. Based on a contextualized study of known security breaches and incidents between 2014 and 2018, my work analyzes the risks of a large-scale instrumentalization of Facebook by private and state actors under a triple hypothesis: (1) such risks worsened or materialized largely as a result of the design and features implemented in the Facebook platform; (2) those features were closely linked to its core business, once defined and successfully exploited; and (3) the policy of acquisitions of companies or services from third parties -Instagram and WhatsApp, among others- reinforced its orientation as a global service under profitability criteria, in detriment of the guarantees for users' privacy and the platform's reliability. Among other results, some aspects linked to the design/management of OSNs with broad social implications are identified, and would require substantial adjustments in the regulatory framework.

PALABRAS CLAVE
Facebook | redes sociales | privacidad | seguridad | control social
KEYWORDS
Facebook | social networks | privacy | security | social control

1. Introducción

Las dinámicas de interacción social se realizan en un grado creciente a través de muy pocas plataformas tecnológicas que operan globalmente en régimen de cuasi-monopolio. Bajo sistemas reguladores heterogéneos, desarrollados por lo general a la medida de sus intereses, estas plataformas han ido integrando servicios y ampliado su funcionalidad hasta constituirse en ecosistemas complejos que atraen y fidelizan a millones de usuarios.

Con un tercio de la población humana entre su base de usuarios, Facebook es sin duda la plataforma más utilizada (1). Integra aplicaciones y servicios tan populares como WhatsApp, Messenger e Instagram (2). La demanda de los servicios que proporciona explica que cuatro de las cinco aplicaciones más descargadas en todo el mundo sean suyas (3). Su mayor base de usuarios está ligada a dispositivos Android (76,2%), a mucha distancia de los demás (15,5% de usuarios de Apple iOS, 8,3% de otros sistemas operativos).

Si en Facebook predominan los hombres en el segmento de usuarios de 18 a 44 años, en Instagram predominan ligeramente las mujeres, sobre todo en el segmento de 18 a 24 años (4). Más acusada en la zona Asia-Pacífico que en Europa y EE.UU-Canadá, su tasa de crecimiento en número total de usuarios mensualmente activos (UAM) y en volumen de negocio ha sido notable en los tres últimos años: de 1.712 millones de usuarios activos/mes y 6.239 millones de dólares de beneficio por publicidad en 2016/Q2 pasó a 2.234 millones de UAM y casi duplicó sus ingresos por publicidad, alcanzando los 13.038 millones de dólares de beneficio en el segundo trimestre de 2018 (5).

Esta evolución coincide con numerosos incidentes y brechas de seguridad que pusieron en riesgo la información personal de decenas de millones de usuarios y facilitaron a ciertos actores, entre 2014 y 2018, el acceso a herramientas y funciones utilizables de modo ilícito. Puesto que coincidieron con períodos decisivos del debate público, que precedieron a cambios relevantes en la dinámica política de

varios países, interesa analizar el fenómeno y determinar el alcance de su impacto. El reducido margen de votantes con el que se logran los nuevos equilibrios entre fuerzas políticas de países como Francia, Estados Unidos, Reino Unido y Alemania, entre otros, ha contribuido a poner el foco de atención en el efecto social a gran escala que pudieran tener eventuales sesgos en el diseño y funcionamiento de plataformas como Facebook (Boshmaf y otros 2013, Ferrara 2017a y 2017b).

Entre la extensa literatura que se ocupa de las redes sociales en línea (OSN), son muchos los trabajos dedicados a explicar por qué han fidelizado a millones de usuarios activos, su rápida consolidación como parte integral del *ecosistema web* actual y los riesgos de su instrumentalización para recolectar datos personales de usuarios, distribuir *malware*, controlar *botnets*, reclutar adeptos y realizar programas de vigilancia masiva (Adewole y otros 2017, Bilogrevic y otros 2016, Ji y otros 2016, Zhang y otros 2017, Benson 2010, Kim y otros 2015, Bhuyan y otros 2017).

Mi trabajo se centra en los riesgos específicos de una instrumentalización de la plataforma Facebook para difundir propaganda y distorsionar el debate público, considerando detalles extraídos de los últimos incidentes y brechas de seguridad conocidos —incluyendo el relativo a Cambridge Analytica— y asumiendo que: 1) tales riesgos se agravaron o materializaron en parte como resultado del diseño y características implementadas en la plataforma Facebook; 2) esas características iban estrechamente ligadas a su núcleo de negocio, una vez definido y explotado con éxito; y 3) la política de adquisiciones de empresas o servicios de terceros —Instagram y WhatsApp, sobre todo— reforzó su orientación como servicio global y facilitó su instrumentalización bajo criterios de rentabilidad, en detrimento de las garantías para la privacidad de los usuarios y la fiabilidad de la plataforma.

Este enfoque refuerza otros resultados de la literatura acerca del caso y aporta elementos adicionales para comprender el potencial de plataformas con las que comparte características para condicionar negativamente la calidad del debate público a diversas escalas. Como conclusión, se destacan aspectos que necesitarían cobertura satisfactoria en un marco regulador diseñado para extender las garantías del debate público convencional a su nueva dimensión tecnológicamente mediada.

2. Antecedentes y elementos comunes con otras OSN

El núcleo de negocio de las redes sociales en línea consiste en captar atención (*eye blowing*) e incrementar de manera sostenida y en poco tiempo su base de usuarios. Es una característica común a las principales OSN conocidas, desde SixDegree (1997) a Facebook, LinkedIn, Instagram, Tumblr o Twitter. Esta última consolidó entre 2006 y enero de 2018 un total de 330 millones de UAM, de los cuales un tercio desarrollan actividad diaria (se publican 500 millones de tweets/día), en su mayoría desde dispositivos móviles (80%) (6).

Su puesta en marcha no requiere inversiones iniciales muy costosas en infraestructura; pero asegurar la fiabilidad del servicio y adoptar las medidas necesarias para prevenir incidentes de seguridad pueden exigir inversiones a gran escala antes incluso de haber consolidado su modelo de negocio. Referidas a Twitter, las cifras de negocio anual —ingresos netos— entre 2010 y 2017 arrojan un saldo negativo ininterrumpido, si bien registra una evolución favorable desde el peor ejercicio (-645 millones de dólares estadounidenses en 2013) hasta 2017 (-108,6 millones de dólares) (7).

Facebook tuvo unos ingresos netos de 3.894 millones de dólares estadounidenses en 2017/Q2, sobre unos ingresos brutos de 9.321 millones de dólares. En 2018/Q2, sus ingresos netos alcanzaron los 5.106 millones de dólares, sobre un total de 13.231 millones de dólares de ingresos brutos (8). Pese a todo, lo relevante en este período ha sido la caída en el número de usuarios en zonas de actividad consolidada, como EE.UU. y Canadá, y la reducción del promedio de horas (50 millones de horas menos) que los usuarios pasan al día en esta red socia (9).

Varios informes recientes apuntan la posibilidad de que el pico de crecimiento en número de usuarios de OSN como Facebook, Twitter y LinkedIn se haya alcanzado en 2017, constatándose a lo largo de 2018 una reducción significativa (-3%), algo mayor en el caso de Facebook (-5%) (10). Al mismo tiempo aumentan ligeramente (2%) los usuarios de Snapchat e Instagram, lo que sugiere la posibilidad de una reorientación de la demanda hacia OSN más centradas en el intercambio de fotos (Pinterest, p.ej., aumenta un 1%) (11). Esta tendencia resulta mucho más acusada en el segmento de edad entre 12-34 años, donde Facebook pierde un 12% de usuarios (sólo pierde un 3% de los usuarios entre 35-54 años). Pero es en el segmento 12-34 donde más aumentan los usuarios de Snapchat e Instagram.

Si bien estudios como los que menciona y desarrolla Taewoo Nam no sustentan la tesis de que la participación política a través de las múltiples herramientas que hacen uso de Internet redunde más en un reforzamiento de las democracias liberales que de los sistemas opresivos con fuertes mecanismos de censura (Nam 2017: 540 y 548), las evidencias de la instrumentalización de Facebook para difundir noticias falsas, vídeos de contenido violento en directo y mensajes con finalidad tóxica durante la campaña presidencial de 2016 en Estados Unidos podrían haber minado de modo irreversible la confianza en este tipo de plataformas (12).

Estos aspectos refuerzan elementos previos de un encuadre negativo más amplio, relativos al modo en que las OSN explotan las vulnerabilidades de la psicología humana para contagiar estados emocionales y secuestrar el tiempo y la atención de millones de usuarios, adictos a una sucesión sin rumbo de

noticias de dudosa credibilidad (Guynn 2018, Kramer y otros 2014, McCarthy 2017).

3. Consolidación y evolución del modelo de negocio

Las OSN se consolidaron a partir de servicios con una reducida base de usuarios, que vinculaban a través de la web a usuarios de una pequeña comunidad: estudiantes de la Universidad de Harvard como germen de Facebook, a partir de una plataforma de juego llamada *Facemash*, donde podían subir fotos y evaluar las de otros; Geocities, como servicio de alojamiento de sitios web para compartir aficiones y conocimientos, que llegó a ser el más exitoso en los años noventa; Friendster, la red social más popular en 2004; o MySpace, lanzado en 2003 y la red social de más éxito entre 2005-2008, con más de 30 millones de visitantes en EE.UU en 2011.

Desde su creación por un grupo de cinco estudiantes de Harvard en 2004, Facebook destacó muy pronto por su popularidad y ritmo vertiginoso de crecimiento: alcanzó 6 millones de usuarios en apenas dos años, y en cuatro llegó a los 100 millones. Esto ocurría en países tan diversos como la India, Alemania, Canadá y EE.UU. Sin apenas herramientas de monetización, no comenzó a ser rentable hasta 2010. En 2012 su valor superaba los 100.000 millones de dólares, y adquirió Instagram por 1.000 millones de dólares. En 2014 destinó 19.000 millones de dólares a la adquisición de WhatsApp, y tres años más tarde su valor como compañía global se estimaba en más de 500.000 millones de dólares (13).

Entre tanto, había resistido las ofertas de adquisición lanzadas por Google, Microsoft o Yahoo. A finales de 2016 eran más de 60 las compañías adquiridas por Facebook, con el objetivo expresamente declarado por Mark Zuckerberg de convertir su empresa en una plataforma global (proyecto *internet.org*), a través de la cual compartir experiencias y comunicar a usuarios de todo el mundo (14). Para entonces, la plataforma había integrado servicios tan diversos como listas de amigos, chats, grupos y páginas, fotos, aplicaciones y juegos, suscripción a contenidos, herramientas de mensajería y videoconferencia.

Una trayectoria de éxito tan sorprendente induce a plantearse qué servicios figuran en su núcleo inicial de negocio y a qué obedece su demanda por parte de usuarios y anunciantes. En esencia, y antes de disponer de herramientas analíticas avanzadas para explotar el resultado de las interacciones de millones de usuarios mediante algoritmos y Big Data, la clave estaba en otorgarle a Facebook “el derecho irrevocable, perpetuo, no exclusivo, transferible y mundial (con la autorización de acordar una licencia secundaria) de utilizar, copiar, publicar, difundir, almacenar, ejecutar, transmitir, escanear, modificar, editar, traducir, adaptar, redistribuir cualquier contenido depositado en el portal” (15).

A la potestad de utilizar a su antojo los contenidos subidos por los usuarios, sin mayores garantías que la autorregulación y versiones poco convincentes de su política de privacidad hasta 2009, pronto agregó la posibilidad de hacer público el rastro de las páginas web visitadas, sin sentirse obligada a eliminar por completo la información generada por aquellos usuarios que decidían darse de baja (16). Los obstáculos que encontraban los usuarios que intentaban darse de baja —en lugar de desactivar temporalmente su cuenta— contrastaban con la facilidad para abrir múltiples perfiles y generar identidades ficticias, como parte de una estrategia continuada de generar expectativas de negocio atrayendo la atención de empresas y anunciantes (17).

Entre 2010 y 2014, Facebook había adquirido tales dimensiones que comenzó a resultar atractiva para actores privados y estatales capaces de explotar algunas de sus características de modo no previsto por los usuarios, incluyendo su instrumentalización para programas de vigilancia masiva (programa *PRISM*, de la Agencia de Seguridad Nacional, NSA, estadounidense), como desveló Edward Snowden en 2013 (Moreno-Muñoz 2014). O para generar campañas de desinformación e intoxicación del debate público mediante el uso de redes de *bots* controlados por actores privados y estatales con cierta capacidad técnica y recursos (Moreno-Muñoz 2017).

4. Brechas de seguridad y vulneración continuada de la privacidad de los usuarios

La plataforma Facebook ha estado funcionando durante años con importantes carencias en materia de seguridad y garantías insuficientes para proteger los datos personales de sus usuarios. En 2011, mucho antes de conocerse la transferencia de 50 millones de registros de usuarios a la controvertida empresa de minería de datos y consultoría política Cambridge Analytica (Moreno-Muñoz 2018: aptdo. 4, notas 11 y 13), la Comisión Federal de Comercio (FTC) estadounidense notificó a Facebook un requerimiento administrativo (*consent order*) para hacer efectiva la protección de la privacidad de los datos de los usuarios. Pero la FTC no puso los medios para asegurar su cumplimiento, y en los años siguientes desistió de hacerlo, aun teniendo constancia de que Facebook trabajaba activamente para evitar su cumplimiento (18).

El requerimiento llegó casi dos años después de que el Electronic Privacy Information Center (EPIC) y una coalición de organizaciones de consumidores registraran una queja ante la FTC, alegando que *Facebook estaba anulando la configuración de las opciones de privacidad establecidas por los usuarios y permitiendo a terceros obtener información privada de los usuarios sin su consentimiento*. Antes de presentar la queja, habían comprobado de manera exhaustiva el alcance del problema y documentado los cambios que la plataforma Facebook introdujo en 2009 en la configuración de las opciones de

privacidad (ibid.).

Al finalizar su investigación, la Comisión Federal de Comercio llegó a un acuerdo global con la empresa en 2011, tras haber determinado el alcance y la gravedad de las malas prácticas desarrolladas:

> "Facebook introdujo cambios en su sitio web para hacer pública cierta información que los usuarios podían haber designado como privada —su Lista de Amigos, p. ej.— sin advertir a los usuarios de este cambio ni obtener su aprobación por adelantado.
>
> La FTC consideró probado en 2011 que Facebook inducía a error a los usuarios que instalaban aplicaciones de terceros, dándoles a entender que esas aplicaciones sólo tendrían acceso a la información imprescindible para funcionar cuando, de hecho, las aplicaciones podían acceder a casi todos los datos personales de los usuarios, y ciertamente a muchos más datos que los necesarios para funcionar.
>
> Aunque el sitio web de Facebook daba a los usuarios la opción de restringir el intercambio de datos a un público limitado ("solo amigos", p. ej.), en la práctica no impidió que su información fuera compartida con aplicaciones de terceros que sus amigos utilizaban. Y esto ocurría porque su programa de aplicaciones verificadas no conseguía garantizar la seguridad de las aplicaciones que los usuarios elegían expresamente por estar verificadas.
>
> Facebook se comprometía con los usuarios a no compartir su información personal con los anunciantes, pero sí lo hacía. Y, aunque Facebook afirmaba que las fotos y vídeos de las cuentas que los usuarios decidían desactivar o eliminar resultaban inaccesibles, en la práctica permitió el acceso al contenido de cuentas desactivadas o eliminadas.
>
> Facebook aseguraba que cumplía con el marco de seguridad (U.S.- EU Safe Harbor Framework) de la UE y los EE.UU. que rige la transferencia de datos entre los EE.UU. y la Unión Europea, pero no lo hizo" (19).

La FTC *prohibió a Facebook seguir haciendo declaraciones falsas sobre la privacidad o seguridad de la información personal de los consumidores y le exigió obtener el consentimiento expreso y afirmativo de aquellos antes de promulgar cambios que anulen sus preferencias de privacidad*, además de adoptar las medidas necesarias para impedir accesos al contenido de un usuario más de 30 días después de haber eliminado su cuenta.

Asimismo, *obligaba a la compañía a establecer y mantener un programa integral de privacidad diseñado para proteger la privacidad y la confidencialidad de la información de los consumidores en la gestión de productos y servicios nuevos y existentes, además de someterse cada dos años a auditorías independientes de terceros que certificaran que cuenta con un programa de privacidad ajustado a los requisitos indicados por la FTC*, capaz de asegurar la protección de la privacidad de la información de los consumidores.

Las deficiencias detectadas por la Comisión Federal de Comercio en su investigación apuntan de forma reiterada al diseño y funciones esenciales sobre las que Facebook articuló su fórmula de negocio: dar acceso a terceros (anunciantes, empresas de marketing y publicidad, aplicaciones) a la información privada de los usuarios, incluso a aquellos contenidos que estos habían decidido mantener como privados o que no eran necesarios para el funcionamiento de ciertas aplicaciones y la prestación del servicio. Pero este tipo de trámites no llevan sanciones aparejadas: solo constatan que la FTC tiene razones para considerar que la ley no se está cumpliendo, subestimando muy probablemente —a la vista del tipo de incidentes de seguridad posteriores— las consecuencias de no haber instado en 2011 un procedimiento sancionador.

5. Alcance del escándalo Cambridge Analytica

En marzo de 2018, los periódicos *The Observer*, *The Guardian* y *The New York Times* denunciaron que Facebook había permitido a la empresa Cambridge Analytica explotar la información personal de más de 50 millones de usuarios de modo contrario a las políticas de privacidad (20) y dando ventaja a ciertos actores para tratar de sesgar la opinión pública en línea con sus intereses.

La información personal se había recolectado a través de una aplicación llamada *thisisyourdigitallife*, construida por Aleksandr Kogan (aunque al margen de su trabajo en la Universidad de Cambridge). A través de su empresa Global Science Research, y en colaboración con Cambridge Analytica, pagó a cientos de miles de usuarios para que se sometieran a un test de personalidad y aceptaron que sus datos fueran recopilados para uso académico. Pero finalmente fueron utilizados fuera de los términos que los usuarios consintieron, y proporcionaron información adicional de la lista de amigos sin su autorización. Los datos obtenidos ilícitamente de Facebook se utilizaron para definir perfiles de votantes en varias campañas electorales y, mediante software avanzado, en combinación con las herramientas de publicidad segmentada implementadas en la plataforma, para predecir e influir en las elecciones (21).

A finales de marzo de 2018, el Reino Unido tenía abiertas dos investigaciones sobre Cambridge Analytica: una de la Electoral Commission, sobre el posible papel de la empresa en el referéndum de la

UE que decantó el resultado hacia el *Brexit*; y otra de la Information Commissioner's Office, sobre el análisis de datos con fines políticos. En Estados Unidos, las acciones de Cambridge Analytica estaban siendo analizadas como parte de la investigación de Robert Mueller sobre la colusión entre D. Trump y Rusia (22).

Las cifras de usuarios afectados varían considerablemente, dependiendo de la fuente y el país afectado. En un comunicado difundido por Mike Schroepfer, responsable de tecnología de Facebook, se cuantificó en 87 millones el total de usuarios a cuyos datos personales habría tenido acceso Cambridge Analytica (23). No se trataba únicamente de metaetiquetas o datos genéricos de uso de servicios:

> "los hackers tuvieron acceso al nombre y datos de contacto (teléfono o correo electrónico) de 15 millones de usuarios. Por otro lado, además de los datos anteriores, también accedieron a los siguientes datos de 14 millones de usuarios: raza, nombre de usuario, género, ubicación, situación sentimental, religión, ciudad de origen, ciudad actual, fecha de nacimiento y los dispositivos desde los que accede a Facebook; educación, trabajo, los últimos lugares donde ha hecho *check-in* o en los que fueron etiquetados y los lugares más buscados por la persona. Por último, existe un millón de usuarios a cuya información no accedieron los hackers, a pesar de que estuvo comprometida" (24).

Los responsable de Cambridge Analytica admitían haber tenido acceso y utilizado esta información para sus fines, aunque limitaban a "unos 30 millones" el número máximo de afectados. Sin embargo, el informante que destapó el caso —Christopher Wylie—, sostuvo en una entrevista para NBC News que podrían ser muchos más de 87 millones (25). Y Mark Zuckerberg, director ejecutivo de Facebook, precisó que el número de afectados en Estados Unidos podría llegar a 70 millones, superar el millón de personas en el Reino Unido, Filipinas e Indonesia; y superar ligeramente los 300.000 usuarios en Australia (26).

6. Otros incidentes de seguridad

Entre 2014 y 2018 numerosos incidentes de seguridad afectaron a la plataforma Facebook. Limitando el análisis a los que comparten elementos con el caso Cambridge Analytica.

A) Prácticas de Crimson Hexagon sobre perfiles de usuarios de Facebook (21/07/2018).

Con sede en Boston, Crimson Hexagon se presenta como una empresa capaz de indagar la percepción de los consumidores (*consumer insights*) con herramientas que le permiten analizar más de 160 millones de fotografías publicadas en línea y más de mil millones de mensajes de medios sociales (Facebook, Instagram, Twitter y otros) todos los días. Entre sus clientes tiene a compañías comerciales como Adidas, Samsung, GM, Walmart y la BBC; pero mantiene contratos de prestación de servicios con agencias gubernamentales de todo el mundo, incluyendo —según *The Wall Street Journal*— una organización rusa sin ánimo de lucro vinculada al Kremlin y varias agencias gubernamentales estadounidenses, además de alguna turca interesada en las reacciones al bloqueo de Twitter en el país (27).

El acceso indebido de Crimson Hexagon a datos personales de usuarios, a pesar del presunto endurecimiento de las políticas de privacidad de Facebook, se había producido también en 2016: afectó sobre todo a usuarios de Instagram, pero por un fallo de seguridad atribuible a Facebook. Por entonces, ni siquiera estaba claro quiénes debían ser los interlocutores en materia de seguridad (28). Con respecto al incidente de 2018, la investigación realizada concluyó que el problema no había adquirido dimensión suficiente como para mantener el bloqueo a las aplicaciones desarrolladas por Crimson Hexagon, y un mes más tarde la compañía retomó su relación comercial con Facebook. Resulta notable el volumen de los contratos que Crimson Hexagon mantenía con diversas agencias gubernamentales, como el Cuartel General de Comunicaciones del Reino Unido (GCHQ). Referido sólo a las estadounidenses, superaba los 800.000 dólares, incluyendo al Departamento de Estado, la Agencia Federal para la Gestión de Emergencias, el ejército, la NSA y otras agencias de inteligencia (29).

B) Prácticas de CubeYou sobre perfiles de usuarios de Facebook (08/04/2018).

Con sede en Nueva York, CubeYou ofrece sus servicios de análisis de perfiles de usuarios con herramientas de inteligencia artificial a marcas comerciales, compañías de medios y agencias. Cuando la CNBC hizo públicas las presuntas malas prácticas, Facebook suspendió la actividad de CubeYou sobre su plataforma y bloqueó el acceso a sus aplicaciones (cuestionarios a través de los cuales recopilaba información sobre los usuarios, supuestamente con finalidad estrictamente académica, aunque la empresa sostiene que su acuerdo le permitía usos más amplios, compatibles con su actividad como empresa especializada en mercadotecnia segmentada). Entre tales usos estaría el *marketing político*, con un alcance superior a los 87 millones de usuarios, de los que manejaba perfiles muy detallados (30). Entre ellos estarían los de unos 137.000 españoles (31).

Una peculiaridad de CubeYou era su capacidad para conectar capas de información mediante potentes herramientas analíticas y de visualización, susceptibles de proporcionar una representación fiable de la mentalidad de los consumidores: comportamiento social en línea en tiempo real, datos de consumo de diversas fuentes —incluyendo *influencers* y *celebrities* de Instagram— y estudios del Censo de los Estados Unidos (32).

C) Prácticas de AggregateIQ (AIQ) durante la campaña del Brexit (07/04/2018).

Con sede en Victoria (Canadá), AIQ se describe como una empresa de sondeo de opinión y marketing político, a domicilio y en línea (33). Habría tenido acceso a un volumen de usuarios similar al que llegaron CubeYou y Cambridge Analytica (la relación con esta última era habitual, según el informante Christopher Wylie), con la finalidad de micro-segmentar las campañas. Facebook bloqueó también el acceso de esta compañía a datos de sus usuarios al revisar parte de la documentación aportada por Wylie (34).

Aparte de intervenir en la campaña del Brexit (prestando servicios para *Vote Leave* y *BeLeave*), habría contribuido presuntamente a difundir propaganda *antiislámica* en los medios sociales antes de las elecciones presidenciales nigerianas de 2015, con el objetivo de desacreditar al candidato de la oposición musulmana que obtuvo la victoria.

En este caso, es destacable el volumen de los contratos gestionados. Según publicó *The Guardian*, *Vote Leave* decidió gastar 3,9 millones de libras esterlinas —más de la mitad de su presupuesto oficial de campaña— en contratar los servicios de AIQ. A esto se suma el gasto de 757.750 libras esterlinas realizado por otras tres asociaciones ideológicamente afines —*BeLeave*, Veteranos por Gran Bretaña y el partido Unionista Democrático—, en una maniobra de *coordinación* entre campañas expresamente prohibida por la ley electoral del Reino Unido, que al parecer concluyó sin que los detalles relativos a la financiación conjunta se facilitaran a la Comisión Electoral (35).

Estos tres casos tienen numerosos elementos en común. Evidencian la carencia de medidas de seguridad, capacidad técnica y recursos humanos con la dimensión necesaria para prevenir incidentes y brechas de seguridad que podían comprometer los datos personales de decenas de millones de usuarios.

7. Limitaciones ligadas al diseño y funcionamiento de los *tokens* en la plataforma

Los incidentes y casos analizados en los apartados anteriores ponen de manifiesto una falta de diligencia continuada por parte de la compañía Facebook para hacer frente a muchas de las amenazas conocidas —propaganda a través de *bots*, campañas de desinformación, episodios coordinados de acoso—, como reconoció Sheryl Sandberg, directora de operaciones de Facebook, ante el Comité del Senado de EE.UU. que investiga la injerencia rusa en la campaña para las elecciones presidenciales de 2016 (36).

Habían transcurrido cinco años desde las exigencias dirigidas por la FTC para mejorar y auditar los procedimientos de seguridad que debían evitar la filtración de datos personales, y M. Zukerberg no aportó mucho más que una petición de perdón por lo ocurrido, en abril de 2018. Sobre los demás aspectos, casi todas las respuestas resultaban evasivas o decepcionantes, incluso presentando medidas recientes como la respuesta adecuada a incidentes de 2015 o anteriores (37).

La mayor vulnerabilidad de todos los servicios integrados en la plataforma Facebook probablemente no consistía en facilitar a agentes extranjeros ejercer una influencia desproporcionada en el modo de pensar de millones de ciudadanos: derivaba de haber consolidado una base tan amplia de usuarios, aglutinados mediante herramientas diseñadas para la mercadotecnia y la publicidad segmentada, que la pusieron en la diana de cualquier actor que pudiera beneficiarse de su instrumentalización para obtener un conocimiento detallado de las preferencias, tendencias y reacciones a ciertos mensajes de un porcentaje suficiente de usuarios por país. Y llevaban prácticamente 10 años funcionando del mismo modo: explotando una misma estrategia de negocio, sustentada en la vulnerabilidad de la información personal de sus 2.200 millones de usuarios (38).

Un componente esencial de esta vulnerabilidad eran las *credenciales de inicio de sesión automatizadas* (*tokens*). Los *tokens* facilitan el acceso a aplicaciones y servicios populares como Spotify, Pinterest o Yelp, a través de una cadena única de letras y números que se puede utilizar para iniciar sesión automáticamente en otras aplicaciones y sitios web, sin necesidad de introducir los datos de usuario y contraseña en cada conexión con estos servicios (39). El fallo asociado con esta vía de *autenticación anidable entre aplicaciones* pudo haber sido explotado desde mucho tiempo atrás (más de un año, con seguridad), y serían vulnerables todos los sistemas similares al utilizado por Facebook, que simplifican de modo parecido el acceso mediante *Single Sign-On* (SSO) —cookies de sesión no protegidas, con frecuencia—, y podrían servir de puerta trasera a miles de aplicaciones y sitios web de terceros (40).

La respuesta de Facebook —anular los *tokens* de 90 millones de usuarios y obligarse a autenticarse de nuevo— no evitaba que las credenciales y direcciones de correo obtenidas con anterioridad volvieran a dar acceso en la mayoría de los intentos (22 de 29, en una de las pruebas). Además, seguía siendo posible suplantar la identidad de muchos usuarios y generar elementos de información que podían mantenerse durmientes hasta que fuese oportuno utilizarlos (41).

Aunque los responsables de seguridad de la plataforma Facebook pudieron minusvalorar el potencial de las herramientas de elusión y hacking disponibles (Callanan y otros 2016), no cabe suponerles desconocimiento de la tendencia constatada entre un alto porcentaje de usuarios a desvelar detalles privados relevantes a cambio de recompensas insignificantes (Kokolakis 2017, Wu y otros 2017,

Preibusch y otros 2016) o por simple narcisismo (Panek y otros 2013, Hallam y Zanella 2017).

Un proceso de autenticación en dos pasos habría sido más eficaz; pero no fue la medida que la plataforma Facebook decidió adoptar. De hecho, cuando intentó algo parecido, arbitró un proceso supuestamente de acceso seguro en varios pasos, consistente en general un *perfil en la sombra* con la información que el usuario no desvelaría nunca (número de teléfono y direcciones de correo electrónico) por motivos de seguridad. Sin que los usuarios tuviesen la menor idea al respecto, Facebook decidió emplear detalles de esta información segura para mejorar la personalización de sus anuncios (*ads*), y facilitar en el proceso el acceso al mismo tipo de información de la red de contactos relacionados. La razón parece obvia: el número de móvil garantiza mayor eficacia en la publicidad dirigida al consumidor y la plataforma no estaba dispuesta a renunciar a esa ventaja (42).

8. Facebook como objetivo del programa de vigilancia electrónica PRISM

Resulta poco verosímil que los servicios de inteligencia con recursos suficientes desistan de llevar a cabo programas de vigilancia masiva cuando tienen a su alcance aplicaciones o herramientas de seguimiento no excesivamente costosas, similares a las que emplean las grandes empresas para sus estudios de mercado (Schuster y otros 2017).

En un contexto de reacciones sociales muy atenuadas al respecto (Stalla-Bourdillon y otros 2014; Reddick y otros 2015) y sin apenas impacto en el valor de mercado de las empresas involucradas (Patsakis y otros 2018), las limitaciones de los procedimientos de seguridad para asegurar la correlación entre identidad física y perfil de usuario en Facebook permiten a diversos actores estrategias muy poderosas de infiltración, como se ha puesto de manifiesto en incidentes posteriores a los comentados en el aptdo. 6 (43).

Aunque los directivos de la compañía suelen declarar en público que *toman muy en serio las acusaciones dirigidas por grupos de defensa de las libertades civiles* —preocupados por los ataques contra disidentes y manifestantes de los que tienen constancia—, y que *no están dispuestos a permitir que los desarrolladores creen herramientas de vigilancia utilizando información de Facebook o Instagram*, lo cierto es que Facebook tiene diversos casos pendientes de resolver en los tribunales por utilizar sus aplicaciones para reunir información sobre los usuarios y sus amigos —incluyendo algunos que no se habían registrado en la red social—, leer sus mensajes de texto, rastrear sus ubicaciones y dar acceso a fotos en sus teléfonos. Así lo entiende Six4Three, en su demanda cursada a través de un tribunal de San Mateo (California), como parte de un caso judicial que dura más de dos años e incluye correos electrónicos confidenciales y mensajes entre altos ejecutivos de Facebook (44).

Los demandantes sostienen que *Facebook continuó explorando e implementando formas de rastrear la ubicación de los usuarios, rastrear y leer sus textos, acceder y grabar con los micrófonos de sus teléfonos, rastrear y monitorear el uso de aplicaciones de la competencia en sus teléfonos, y rastrear y monitorizar sus llamadas* (ibid., traducción propia). Para lograr su propósito habrían desarrollado herramientas específicas para sistemas Android o iOS, según marcas y tipos de teléfonos móviles.

Estos detalles resultan consistentes con las características del programa PRISM (en clave, SIGAD US-984XN) desplegado por la NSA, sus colaboradores del GCHQ en el Reino Unido y otras agencias de inteligencia, según reveló Edward Snowden en 2013 (45). PRISM es un programa clandestino de vigilancia electrónica y minería de datos desarrollado por la NSA al menos desde el año 2007. Incluye herramientas avanzadas de interceptación y permite extraer datos de las comunicaciones por Internet registradas en los servidores de empresas como Google Inc. y Apple Inc. que coinciden con los términos de búsqueda aprobados por el tribunal de Vigilancia de Inteligencia Extranjera FISA (conforme a la sec. 702 de la Enmienda a la Ley FISA de 2008) (46).

El procedimiento permite a la NSA acceder a comunicaciones cifradas en su tránsito por los nodos troncales de Internet y obtener datos relativamente fáciles de manejar, aunque con frecuencia origina falsos positivos y pueden desencadenar actuaciones injustas, abusivas o desproporcionadas. Snowden denunció que la recopilación de datos tenía un carácter masivo y tipificable como actividad criminal, según la información difundida por *The Guardian* y *The Washington Post* el 6 de junio de 2013 (47).

Las agencias y socios involucrados en el programa PRISM tenían un acuerdo financiero de cientos de millones de dólares (cada año de funcionamiento tendría un coste aproximado de 20 millones de dólares estadounidenses). Se consideraba la principal fuente de datos brutos de inteligencia para los informes analíticos de la NSA y estaba diseñado para superar las restricciones existentes relativas a la recopilación de datos para la lucha anti-terrorista. A través de una presentación interna fechada en abril de 2013 y filtrada por Snowden se supo que permite acceder a mensajes de correo electrónico, videoclips, fotos y llamadas de voz y vídeo, datos de redes sociales, e inicios de sesión y otros datos de acceso a los servicios prestados por una larga serie de empresas de Internet en Estados Unidos: Microsoft y su división de Skype; Google y su división YouTube; Yahoo, Facebook, AOL y Apple, entre otras (Moreno-Muñoz 2014, Hoskins 2017: 2 y 4).

Sin embargo, es probable que la instrumentalización de Facebook para programas de vigilancia masiva resulte de menor alcance que la conseguida en relación con empresas de comunicaciones como Comcast, AT&T y Verizon, que para muchos usuarios resultan más difíciles de soslayar como

intermediarios en la prestación de servicios (48).

9. Nueva brecha de seguridad con decenas de millones de usuarios afectados

El incidente de mayor gravedad que ha afectado a la plataforma Facebook en sus 14 años de existencia fue descubierto a finales de septiembre de 2018, y pudo afectar a más de 50 millones de usuarios (incluyendo a varios de sus principales directivos) (49).

Los atacantes explotaron una característica del código —un error en el programa de carga de vídeos para las celebraciones de cumpleaños— que da acceso a las cuentas de usuario y habría posibilitado tomar el control de las mismas. Esta funcionalidad se había introducido en julio de 2017, y explotaba igualmente los *tokens* de acceso. Como se indicó en el aptdo. 7, la medida adoptada por la compañía —desactivar temporalmente las credenciales de inicio de sesión de más de 90 millones de usuarios— no suprime el riesgo de que se repitan incidentes de alcance similar (50).

Los hackers pudieron obtener información privada muy detallada de los usuarios (nombre, sexo y ciudad natal, p. ej.) y conocer todo lo que había en el perfil de las víctimas, aunque no se había podido determinar el alcance del acceso a las cuentas de terceros. Es obvio que los recursos destinados *a integrar la seguridad en cada paso del desarrollo de productos de Facebook* no habían dado el resultado esperado, aunque en este caso se trató de un ataque muy sofisticado, que consiguió explotar lo que Guy Rosen —vicepresidente de producto de Facebook— describió como "una interacción compleja de múltiples *bugs"* (Matsakis y Lapowsky 2018). En realidad, parece más bien otra forma hábil de explotar la vulnerabilidad de los *tokens* asociada con la función "View as".

Quizá no resulte muy realista esperar de una compañía cuyo negocio depende de la eficacia de su sistema para dirigir publicidad segmentada mayor diligencia en la adopción de medidas de seguridad que garanticen la privacidad de sus 2.000 millones de usuarios, en cada uno de los países donde presta servicios, conforme al requerimiento de la Comisión Federal de Comercio estadounidense en 2011. Pero es obvio que Facebook no hizo durante años lo suficiente para incentivar la adopción de buenas prácticas de privacidad (Wang y otros 2019, Kwon y otros 2014, Tormo y otros 2015).

En junio de 2018, Facebook reconoció tener constancia de un "error" que pudo permitir el acceso público a los mensajes de 14 millones de usuarios durante días (51). Pero fue a finales de septiembre cuando admitió por primera vez que todo el contenido de las cuentas de decenas de millones de usuarios pudo haber sido accesible a hackers extranjeros. Incluso aunque el incidente fuera de alcance limitado, la información obtenida podría ser utilizada más adelante para sortear sistemas de autenticación de varios pasos y operar de forma fraudulenta con perfiles falsos (52).

10. Conclusiones

En lugar de contribuir a la alfabetización de sus usuarios en materia de ciberseguridad y garantías para la privacidad, muchas noticias sobre vulnerabilidad y acceso indebido a datos privados de Facebook tenían que consultarse a través de Twitter, búsquedas de Google y otros sitios en línea, porque la compañía decidió retirar las entradas y mensajes procedentes de *The Guardian* y *The Associated Press*, entre otras fuentes. La actividad de miles de usuarios publicando historias al respecto resultó sospechosa para los sistemas de filtrado que Facebook emplea para prevenir el uso abusivo su red (53).

Aunque Facebook no ha logrado por el momento implementar medidas eficaces para protegerse contra la injerencia de terceros en campañas electorales ni garantizar que los usuarios tengan su información personal bajo control, sus directivos declaran estar dispuestos a esmerarse hasta conseguir que sus herramientas de inteligencia artificial consigan censurar los discursos de odio y los llamamientos a la violencia. Han logrado, sin embargo, resultados sorprendentes en la censura de desnudos femeninos (54).

Sus tiempos de reacción han sido muy lentos, en general. En varios incidentes graves habría sobrepasado las 72 horas que el nuevo Reglamento General de Protección de Datos (GDPR) da de plazo a las empresas para que revelen los incidentes de seguridad a las agencias europea concernidas (y en caso de riesgo importante, seguido de notificaciones directas a los usuarios). Otros se habrían mantenido en secreto durante meses, de no ser por la actividad de los informantes.

La reacción de Facebook a sus múltiples incidentes de seguridad y su trayectoria como empresa ilustran con claridad los riesgos de toda prestación de servicios digitales globales en régimen de cuasi-monopolio. Ejemplifica también los límites de la autorregulación como garantía de seguridad, cuando el núcleo de negocio va ligado al aumento constante del número de usuarios y al tipo de información detallada a la que consiguen acceder los anunciantes para optimizar la eficacia de sus herramientas de publicidad segmentada.

La versatilidad de estas herramientas, instrumentalizables tanto para mercadotecnia convencional como para estrategias de acoso, desinformación y propaganda política, atrajo inversiones, capacidad profesional y talento en una proporción mucho mayor que la destinada a las herramientas de analítica y

recursos humanos para curaduría de contenidos (Giles 2011). Sus prioridades se centraban en sumar y retener usuarios, incrementando con herramientas de gran poder adictivo el número de horas que pasaban en los distintos servicios de la plataforma, más que en asegurar la privacidad de sus interacciones y reforzar la infraestructura de seguridad de la plataforma (McCarthy y otros 2016).

Sin un marco regulador adecuado, orientado a establecer mecanismos de rendición de cuentas similares a los que limitan las acciones de otros actores durante períodos decisivos del debate público, será inevitable que las malas prácticas frecuentes en las contiendas electorales se sigan desplazando a plataformas como Facebook. Resultan idóneas para ampliar su alcance y desarrollar herramientas de prospectiva y control social, con la posibilidad de conectar capas de información sin consentimiento de los usuarios. Semejante esquema de monetización de datos puede afectar a principios democráticos fundamentales, como el de imparcialidad (M-Bascuñán 2018).

La distorsión en los cauces de acceso a la información para intoxicar el espacio público con elementos que, por su propio funcionamiento y sin conocimiento de los usuarios, imponen la tiranía de las emociones al ejercicio de la razón, desde plataformas o servicios que permiten fusionar identidades ficticias y reales, constituye un ingrediente muy común en las distopías tecnológicas de la era de Internet (Goertzel y otros 2017, Holder y otros 2016). El riesgo de que se materialice aumenta referido a plataformas de titularidad privada que gestionan los datos personales de millones de usuarios y amplían su margen de beneficio mediante publicidad segmentada, o vendiendo a terceros la información sobre patrones de comportamiento e interacciones de sus usuarios (Schuster y otros 2017).

Sin instrumentos transfronterizos de gobernanza, como base para el desarrollo de marcos reguladores consistentes y mecanismos sancionadores disuasorios, no cabe esperar que un reducido grupo de Estados consiga evitar abusos como los producidos por los múltiples actores privados y estatales que han conseguido explotar las vulnerabilidades de los servicios y aplicaciones integrados en la plataforma Facebook.

Notas

1. Facebook tenía 2.230 millones de usuarios activos (aquellos que inician sesión al menos una vez al mes) en el segundo trimestre de 2018. En 2012 alcanzó los mil millones de usuarios activos, siendo la primera red social que alcanzaba esa cifra. Además de ser la plataforma de red social más popular del mundo —la que más se le aproxima es YouTube, con 1.500 millones de usuarios activos—, es la que cuenta con mayor base de usuarios que acceden desde dispositivos móviles (1.740 millones). Cfr. https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q2/Q2-2018-Earnings-Presentation.pdf; https://www.omnicoreagency.com/facebook-statistics. [Todos los enlaces del texto seguían activos a fecha 02/11/2018.]

2. Cfr. Digital 2018, pág. 59 (con datos de enero de 2018): https://www.juancmejia.com/wp-content/uploads/2014/02/Estudio-de-estad%C3%ADsticas-de-Internet-y-Redes-Sociales-WeAreSocial-y-Hootsuite.pdf.

3. Ibid., pág. 121.

4. Véase nota 2, pág. 77.

5. Cfr. *Facebook Q2 2018 Results*, disponible en: https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q2/Q2-2018-Earnings-Presentation.pdf

6. La evolución y estadísticas de uso de Twitter convergen en varios aspectos con las indicadas para la plataforma Facebook en nota 1: 34% de usuarios masculinos, frente a un 21% de usuarias; 37% de usuarios entre los 18 y 29 años de edad; 25% entre 30 y 49 años. Cfr. https://www.flimper.com/blog/es/estadisticas-globales-de-twitter-2018-.

7. En España, la red social Twitter declaró un beneficio neto de 290.548 euros en España. Cfr. https://es.statista.com/estadisticas/513568/twitter-ingresos-netos-anuales/.

8. Cfr. https://s21.q4cdn.com/399680738/files/doc_financials/2017/Q4/Q4-2017-Earnings-Presentation.pdf;

https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q2/Q2-2018-Earnings-Presentation.pdf

9. Cfr. https://www.abc.es/tecnologia/redes/abci-facebook-frenazo-crecimiento-facebook-primera-pierde-numero-usuarios-201802010931_noticia.html;

10. Cfr. *The Infinite Dial 2018*, de Edison Research and Triton Digital, en https://www.slideshare.net/webby2001/infinite-dial-2018 (pág. 16). También https://eu.usatoday.com/story/tech/2018/01/31/mark-zuckerberg-people-spending-50-million-fewer-hours-facebook-reduced-time-people-spend-50-million/1081082001/.

11. Ibid., pág. 18.

12. Cfr. algunos titulares al respecto: “European elections ‘face growing threat of manipulation’” (https://www.theguardian.com/technology/2018/oct/23/risk-of-interference-in-mep-elections-growing-eu-commission-facebook-scandal-monitoring); “Facebook apologises for psychological experiments on users” (https://www.theguardian.com/technology/2014/jul/02/facebook-apologises-psychological-experiments-on-users); “Facebook reveals news feed experiment to control emotions” (https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds); “Facebook sorry – almost – for secret psychological experiment on users” (https://www.theguardian.com/technology/2014/oct/02/facebook-sorry-secret-psychological-experiment-users); “Facebook and Twitter are being used to manipulate public opinion – report” (https://www.theguardian.com/technology/2017/jun/19/social-media-proganda-manipulating-public-opinion-bots-accounts-facebook-twitter); “How Russia used social media to divide Americans” (https://www.theguardian.com/us-news/2017/oct/14/russia-us-politics-social-media-facebook).

13. Cfr. http://www.ticbeat.com/socialmedia/la-historia-de-facebook-desde-2004-hasta-hoy/.

14. Cfr. http://www.ticbeat.com/empresa-b2b/la-carta-de-zuckerberg-hagamos-de-facebook-la-solucion-a-los-muros/.

15. Cfr. https://es.wikipedia.org/wiki/Facebook#cite_ref-40.

16.
Cfr. https://web.archive.org/web/20100616151127/http://mx.news.yahoo.com/s/afp/100506/tecnologia/eeuu_tecnolog__a_internet; https://www.huffingtonpost.com/ari-melber/does-facebook-own-you-for_b_86115.html?guccounter=1.

17. Véanse, entre otros, los titulares siguientes: “La misión imposible de eliminar y dar de baja tu perfil de Facebook”, en

https://www.abc.es/tecnologia/redes/abci-como-eliminar-o-desactivar-cuenta-facebook-201803192131_noticia.html;

“Cómo borrar tu cuenta de Facebook por completo y para siempre”, en https://www.genbeta.com/paso-a-paso/como-borrar-tu-cuenta-de-facebook-por-completo-y-para-siempre; “How To Permanently Delete A Facebook Account”, en https://deletefacebook.com/; “How to permanently delete your Facebook account”, en https://www.telegraph.co.uk/technology/0/permanently-delete-facebook-account/; “How to delete a Facebook account permanently in 3 simple steps”, en https://www.trustedreviews.com/news/how-to-delete-facebook-account-2950145.

18. Cfr. Rotenberg, M. (2018). “How the FTC Could Have Prevented the Facebook Mess”, en https://techonomy.com/2018/03/how-the-ftc-could-have-avoided-the-facebook-mess/.

19. Traducción y elementos en cursiva míos. Texto original en inglés disponible en: Federal Trade Commission (November 29, 2011): “Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises”. https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

20. Sobre la ambigüedad de las políticas de privacidad de Facebook y su inadecuación para fomentar prácticas de interacción en línea seguras y una cultura de privacidad más sofisticada, véanse: Child y Starcher 2016; Moreno-Muñoz 2018.

21. Cfr. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election; https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump; https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html; https://www.nytimes.com/es/2018/04/04/facebook-cambridge-analytica-87-millones/; https://observer.com/2018/04/ex-cambridge-analytica-director-speaks-out-on-facebook-scandal/.

22. Cfr. Cadwalladr, C., & Graham-Harrison, E. (March 17, 2018). “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach”. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

23. Cfr. https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach; https://www.muycomputer.com/2018/04/05/facebook-cambridge-analytica/.

24. Cfr. http://www.enter.co/cultura-digital/redes-sociales/facebook-fue-hackeado-otra-vez/#! (traducción propia).

25. Cfr. https://www.nbcnews.com/meet-the-press/video/misused-data-from-facebook-users-could-absolutely-be-higher-than-87-million-cambridge-analytica-co-founder-says-1205345347991?v=raila&.

26. Cfr. https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach.

27. Cfr. https://www.bbc.com/news/technology-44909293; https://www.wsj.com/articles/facebook-probing-how-analytics-firm-shares-public-user-data-1532104502;

https://www.theguardian.com/technology/2018/jul/20/facebook-crimson-hexagon-analytics-data-surveillance.

28. Cfr. https://www.theguardian.com/technology/2018/jul/20/facebook-crimson-hexagon-analytics-data-surveillance.

29. Cfr. nota 28 y https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

30. Cfr. https://www.cnbc.com/2018/04/08/cubeyou-cambridge-like-app-collected-data-on-millions-from-facebook.html;

31. Cfr. https://www.abc.es/tecnologia/redes/abci-facebook-admite-relaciones-segunda-empresa-similar-cambridge-analytica-201804091748_noticia.html.

32. Cfr. http://www.cubeyou.com (consultada: 1/11/2018).

33. Cfr. https://aggregateiq.com (consultada: 1/11/2018).

34. Cfr. https://www.bbc.com/news/technology-43680969.

35. Cfr. https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

36. Cfr. https://elpais.com/internacional/2018/09/05/actualidad/1536149279_373038.html;

https://www.xataka.com/privacidad/fue-mi-error-y-lo-siento-yo-inicie-facebook-y-yo-soy-responsable-de-lo-que-pasa-aqui-mark-zuckerberg-ante-el-congreso-de-eeuu.

37. Cfr. https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf.

38. Cfr. https://elpais.com/internacional/2018/04/10/actualidad/1523380980_341139.html.

39. Cfr. https://www.theguardian.com/technology/2018/oct/02/facebook-hack-compromised-accounts-tokens. Sobre *implicit authentication* y su posible explotación para acceder a información de perfiles de usuario, véase Shahandashti y otros 2015.

40. Cfr. las aportaciones sobre el tema de Jason Polakis y otros expertos en ciencias de la computación de la Universidad de Illinois en Chicago: https://www.cs.uic.edu/~polakis/papers/sso-usenix18.pdf. Por otra parte, el uso de herramientas potentes de encriptación puede suponer un sobrecoste importante y ralentizar el funcionamiento de los sistemas y servicios, como señalan Yan y otros 2016.

41. Cfr. https://www.theguardian.com/technology/2018/oct/02/facebook-hack-compromised-accounts-tokens.

42. Cfr. https://www.gizmodo.com.au/2018/09/facebook-is-giving-advertisers-access-to-your-shadow-contact-information/; https://www.inquisitr.com/5090902/facebook-2-factor-authentication-security-advertising/. Los detalles se conocieron a finales de septiembre de 2018.

43. Cfr. “Facebook removes 652 fake accounts and pages meant to influence world politics” (*The Guardian*,

21/08/2018): https://www.theguardian.com/technology/2018/aug/21/facebook-pages-accounts-removed-russia-iran; “Facebook Removes More Accounts Tied to Iran – Company says pages were part of an effort to post ‘inauthentic’ information ahead of the U.S. midterm elections” (*The Wall Street Journal*, 26/10/2018), en: https://www.wsj.com/articles/facebook-removes-more-accounts-tied-to-iran-1540576002.

44. Cfr. https://www.theguardian.com/technology/2018/may/24/facebook-accused-of-conducting-mass-surveillance-through-its-apps.

45. Cfr. https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google; http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/;

46. Cfr. https://www.congress.gov/bill/110th-congress/house-bill/6304.

47. Cfr. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/;

48. Cfr. https://www.theguardian.com/commentisfree/2018/apr/06/delete-facebook-live-us-still-share-data.

49. Cfr. https://newsroom.fb.com/news/2018/09/security-update/; https://www.itnews.com.au/news/facebook-security-breach-affects-50-million-users-513280.

50. Cfr. https://www.cbc.ca/news/technology/facebook-data-breach-1.4842815.

51. Cfr. https://www.nytimes.com/2018/06/07/technology/facebook-privacy-bug.html; https://eu.usatoday.com/story/tech/2018/06/07/facebook-bug-changed-14-m-users-privacy-statuses-public/682494002/.

52. Cfr. http://www.digitaljournal.com/internet/significance-of-facebook-data-breach-explained-interview/article/533269.

53. Cfr. https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

54. Cfr. https://elpais.com/elpais/2018/09/17/opinion/1537198097_058194.html.

Bibliografía

Adewole, K. S. (y otros)
2017 "Malicious accounts: Dark of the social networks", *Journal of Network and Computer Applications*, nº 79: 41-67. https://doi.org/http://dx.doi.org/10.1016/j.jnca.2016.11.030

Benson, J. P.
2010 "Cyber Threats: An Emerging Concern", en K. Kerr (ed.), *Workplace Violence*. Boston, Elsevier: 215-234.
https://doi.org/10.1016/B978-1-85617-698-9.00015-1

Bhuyan, S. S. (y otros)
2017 "Privacy and security issues in mobile health: Current research and future directions", *Health Policy and Technology*.
https://doi.org/10.1016/j.hlpt.2017.01.004

Bilogrevic, I. (y otros)
2016 "A machine-learning based approach to privacy-aware information-sharing in mobile social networks", *Pervasive and Mobile Computing*, nº 25: 125-142. https://doi.org/10.1016/j.pmcj.2015.01.006

Boshmaf, Y. (y otros)
2013 "Design and analysis of a social botnet". *Computer Networks*, nº 57 (2): 556-578. http://dx.doi.org/10.1016/j.comnet.2012.06.006

Callanan, C. (y otros)
2016 "User awareness and tolerance of privacy abuse on mobile Internet: An exploratory study", *Telematics and Informatics*, nº 33 (1): 109-128.
https://doi.org/10.1016/j.tele.2015.04.009

Child, J. T. (y S. C. Starcher)
2016 "Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management", *Computers in Human Behavior*, nº 54: 483-490.
https://doi.org/10.1016/j.chb.2015.08.035

Ferrara, E.
2017a "Disinformation And Social Bot Operations In The Run Up To The 2017 French Presidential Election".
https://arxiv.org/ftp/arxiv/papers/1707/1707.00086.pdf

2017b "Contagion Dynamics of Extremist Propaganda in Social Networks", *SSRN Electronic Journal*.
https://doi.org/10.2139/ssrn.2982259

Giles, J.
2011 "Inside Facebook's massive cyber-security system". *New Scientist*, nº 212 (2836): 21-22.
https://dx.doi.org/10.1016/S0262-4079(11)62643-2

Goertzel, B. (y otros)
2017 "The global brain and the emerging economy of abundance: Mutualism, open collaboration, exchange networks and the automated commons", *Technological Forecasting and Social Change*, nº 114: 65-73.
https://doi.org/10.1016/j.techfore.2016.03.022

Guynn, J.
2018 "Mark Zuckerberg: People are spending 50 million fewer hours on Facebook a day", *USA TODAY*, 31/01/2018.
https://eu.usatoday.com/story/tech/2018/01/31/mark-zuckerberg-people-spending-50-million-fewer-hours-facebook-reduced-time-people-spend-50-million/1081082001/

Hallam, C. (y G. Zanella)
2017 "Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards", *Computers in Human Behavior*, nº 68. 217-227.

https://doi.org/10.1016/j.chb.2016.11.033

Holder, C. (y otros)
2016 “Robotics and law: Key legal and regulatory implications of the robotics age (part II of II)”, *Computer Law & Security Review*, nº 32 (4): 557-576.
https://doi.org/10.1016/j.clsr.2016.05.011

Hoskins, A.
2017 “Risk media and the end of anonymity”, *Journal of Information Security and Applications*.
https://doi.org/10.1016/j.jisa.2017.01.005

Ji, Y. (y otros)
2016 “Combating the evasion mechanisms of social bots”, *Computers & Security*, nº 58: 230-249.
https://doi.org/10.1016/j.cose.2016.01.007

Kim, E. (y otros)
2015 “Design and analysis of enumeration attacks on finding friends with phone numbers: A case study with KakaoTalk”, *Computers & Security*, nº 52: 267-275.
https://doi.org/http://dx.doi.org/10.1016/j.cose.2015.04.008

Kokolakis, S.
2017 “Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon”, *Computers & Security*, nº 64: 122-134.
https://doi.org/10.1016/j.cose.2015.07.002

Kramer, A. D. I. (y otros)
2014 “Experimental evidence of massive-scale emotional contagion through social networks”, *Proceedings of the National Academy of Sciences*, 111 (24): 8788-8790.
https://doi.org/10.1073/pnas.1320040111

Kwon, S. J. (y otros)
2014 “What drives successful social networking services? A comparative analysis of user acceptance of Facebook and Twitter”, *The Social Science Journal*, nº 51 (4): 534-544.
https://doi.org/10.1016/j.soscij.2014.04.005

M-Bascuñán, M.
2018 “Controladores sin control”, *El País*, 07/04/2018.
https://elpais.com/elpais/2018/04/06/opinion/1523014815_288419.html

Matsakis, L. (y I. Lapowsky)
2018 “Everything We Know About Facebook’s Massive Security Breach”, *Wired,* 28/09/2018.
https://www.wired.com/story/facebook-security-breach-50-million-accounts/

McCarthy, O. T. (y otros)
2016 “Technology engagement and privacy: A cluster analysis of reported social network use among transport survey respondents”, *Transportation Research Part C: Emerging Technologies*, nº 63: 195-206.
https://doi.org/10.1016/j.trc.2015.12.015

McCarthy, T.
2017 “How Russia used social media to divide Americans”, *The Guardian,* 14/10/2017.
https://www.theguardian.com/us-news/2017/oct/14/russia-us-politics-social-media-facebook

Moreno-Muñoz, M.
2014 “El caso Snowden”, *La Maleta de Portbou – Revista de Humanidades y Economía*, nº 4: 86-91.
http://www.lamaletadeportbou.com/products-page/revistas/4-marzo-abril-2014/
2017 “Privacidad y procesado automático de datos personales mediante aplicaciones y bots”. *Dilemata: Revista Internacional de Éticas Aplicadas / International Journal of Applied Ethics*, nº 9 (24): 1-23.
http://www.dilemata.net/revista/index.php/dilemata/article/download/412000098/488

Moreno Muñoz, M.
2018 “Virtualización del espacio público y concepto débil de privacidad. Lecciones del caso Facebook-Cambridge Analytica”, *Ensayos de Filosofia*, nº 8/2 (3).
http://www.ensayos-filosofia.es/archivos/articulo/virtualizacion-del-espacio-publico-y-concepto-debil-de-privacidad-lecciones-del-caso-facebook-cambridge-analytica

Nam, T.
2017 “A tool for liberty or oppression? A cross-national study of the Internet’s influence on democracy”, *Telematics and Informatics*, nº 34 (5): 538-549.
https://doi.org/10.1016/j.tele.2016.11.004

Panek, E. T. (y otros)
2013 “Mirror or Megaphone?: How relationships between narcissism and social networking site use differ on Facebook and Twitter”, *Computers in Human Behavior*, nº 29 (5): 2004-2012.
https://doi.org/10.1016/j.chb.2013.04.012

Patsakis, C. (y otros)
2018 “The market’s response toward privacy and mass surveillance: The Snowden aftermath”, *Computers & Security*, nº 73: 194-206.
https://doi.org/https://doi.org/10.1016/j.cose.2017.11.002

Preibusch, S. (y otros)
2016 “Shopping for privacy: Purchase details leaked to PayPal”, *Electronic Commerce Research and Applications*, nº 15: 52-64.
https://doi.org/10.1016/j.elerap.2015.11.004

Reddick, C. G. (y otros)
2015 “Public opinion on National Security Agency surveillance programs: A multi-method approach”, *Government Information Quarterly*, nº 32 (2): 129-141.
https://doi.org/http://dx.doi.org/10.1016/j.giq.2015.01.003

Schuster, S. (y otros)
2017 “Mass surveillance and technological policy options: Improving security of private communications”, *Computer Standards & Interfaces*, nº 50, 76-82.
https://doi.org/10.1016/j.csi.2016.09.011

Shahandashti, S. F. (y otros)
2015 “Reconciling user privacy and implicit authentication for mobile devices”, *Computers & Security*, nº 53: 215-233.
https://doi.org/10.1016/j.cose.2015.05.009

Stalla-Bourdillon, S. (y otros)
2014 “From porn to cybersecurity passing by copyright: How mass surveillance technologies are gaining legitimacy… The case of deep packet inspection technologies”, *Computer Law & Security Review*, nº 30 (6): 670-686.
https://doi.org/http://dx.doi.org/10.1016/j.clsr.2014.09.006

Tormo, G. D. (y otros)
2015 “Towards privacy-preserving reputation management for hybrid broadcast broadband applications”, *Computers & Security*, nº 49: 220-238. https://doi.org/http://dx.doi.org/10.1016/j.cose.2014.10.010

Wang, H. (y otros)
2019 “Privacy-preserving incentive and rewarding scheme for crowd computing in social media”, *Information Sciences*, nº 470: 15-27.
https://doi.org/10.1016/j.ins.2018.07.016

Wu, E. (y otros)
2017 “Confidentiality and Privacy for Smartphone Applications in Child and Adolescent Psychiatry: Unmet Needs and Practical Solutions”, *Child and Adolescent Psychiatric Clinics of North America*, nº 26 (1): 117-124.
https://doi.org/10.1016/j.chc.2016.07.006

Yan, Z. (y otros)
2016 “Two Schemes of Privacy-Preserving Trust Evaluation”, *Future Generation Computer Systems*, nº 62: 175-189.
https://doi.org/10.1016/j.future.2015.11.006

Zhang, S. (y otros)
2017 “Secure hitch in location based social networks”, *Computer Communications*, nº 100: 65-77.
https://doi.org/10.1016/j.comcom.2017.01.011