



UNIVERSIDAD
DE GRANADA

XIX Semana de Ética y Filosofía Política (AEEFP)
Congreso Internacional AEEFP-SIEU 2018
El Ferrol, 5/10/2018

Mesa 23: Big Data

Por qué las políticas de privacidad de Facebook no evitaron el abuso de Cambridge Analytica

Miguel Moreno Muñoz
mm3@ugr.es

Contenido

- **Facebook y su modelo de negocio**
 - Núcleo de negocio: atraer atención (eye blowing)
 - Poco gasto en infraestructura (pero requiere inversión escalar)
- **Antecedentes**
 - Servicios similares con menos usuarios, sin herramientas de monetización
 - Pocas herramientas analíticas, algoritmos y AI para big data
 - Programas de vigilancia masiva al alcance de muy pocos actores estatales/privs.
- **Autorregulación y múltiples brechas de seguridad**
 - Desafíos recientes no previstos → injerencia rusa, fake news, distorsión electoral
 - Problemas para asegurar la correlación identidad física-virtual
 - Bots/botnets sofisticados, instrumentalizables por trolls con conocimientos básicos
 - Base de usuarios con masa crítica para impacto político y social dirigido
 - Muchas opciones de privacidad para usuarios; poca infraestructura de seguridad.

Ideas centrales

- **Paradoja: de servicio lúdico a infraestructura esencial en la virtualización del debate público**
 - Acentuado por la **digitalización** e incorporación de **inteligencia artificial** en tareas de curaduría/supervis.
 - **Un modelo de negocio con limitada competencia**
 - **Otras plataformas muy segmentadas**
 - **Fuente de ingresos** muy dependiente de la atracción de nuevos usuarios y de cómo focalizar su atención.
 - “El **modelo de negocio se basa en hacer crecer el número de usuarios y las conexiones e interacciones entre ellos** para, de esa forma, aumentar su base de datos”

Sandy Parakilas, ex responsable de operaciones en Facebook

1. Expansión y consolidación

Posición de dominio en el mercado por adquisición/integración de competidores

Una posición de cuasi-monopolio

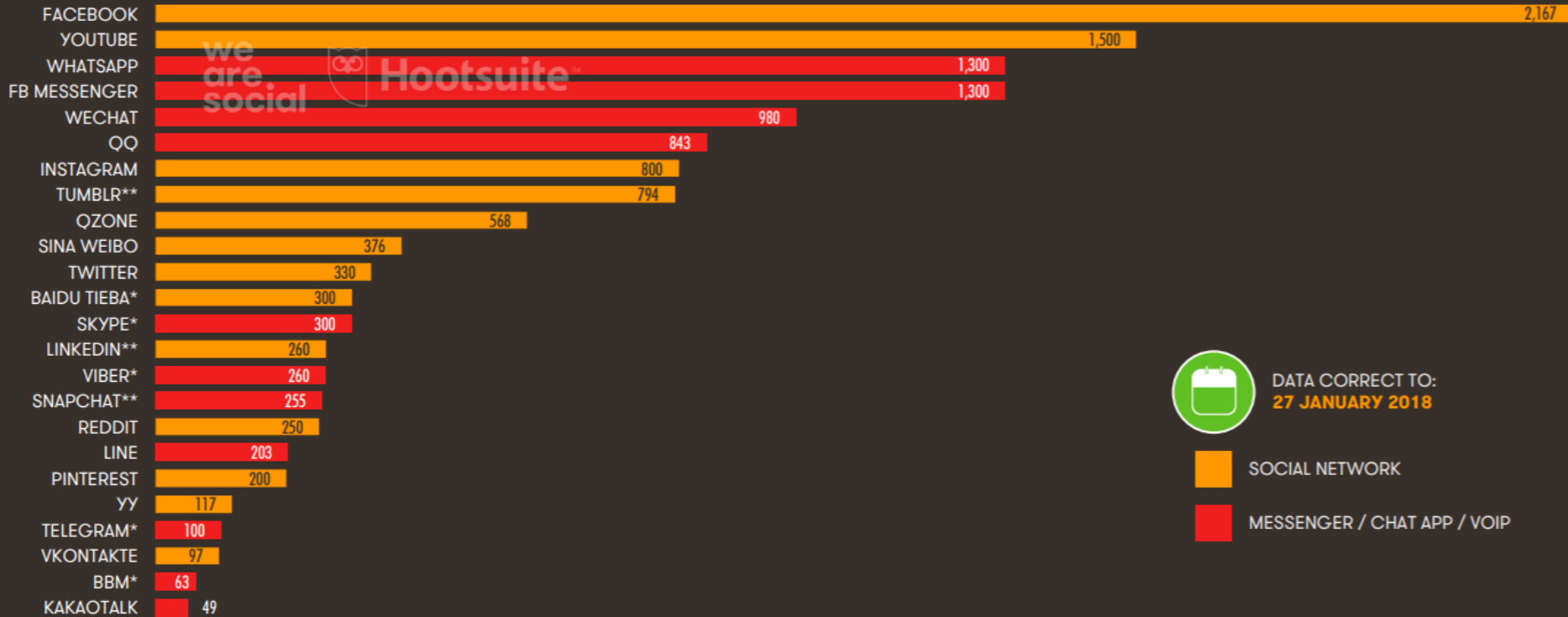
12/04/2018: <https://elcomercio.pe/tecnologia/redes-sociales/facebook-mark-zuckerberg-dueno-clona-8-apps-llama-competencia-noticia-511446>

- **Facebook posee tres de las 10 principales aplicaciones en la tienda de iOS en EE.UU.**
 - **Instagram** (puesto 4),
 - **Messenger** (puesto 6)
 - **Facebook** (puesto 8).
 - Facebook está desarrollando su **pestaña Watch para competir con YouTube** (puesto 5) y **ha clonado a Snapchat** (puesto 7).
- Es intrigante que el Congreso no haya tramitado ninguna iniciativa para dividir **Facebook, Instagram y WhatsApp**.
 - Como empresas independientes, cada usuario podría elegir dónde depositar sus datos, evitando que una misma plataforma los comparta.
 - La estructura de aplicaciones múltiples de **Facebook** crea **economías de escala en los datos** para compartir objetivos de anuncios y equipos de ventas, trabajos en ingeniería y algoritmos de clasificación de relevancia.

JAN
2018

ACTIVE USERS OF KEY GLOBAL SOCIAL PLATFORMS

BASED ON THE MOST RECENTLY PUBLISHED MONTHLY ACTIVE USER ACCOUNTS FOR EACH PLATFORM, IN MILLIONS



DATA CORRECT TO:
27 JANUARY 2018



SOCIAL NETWORK



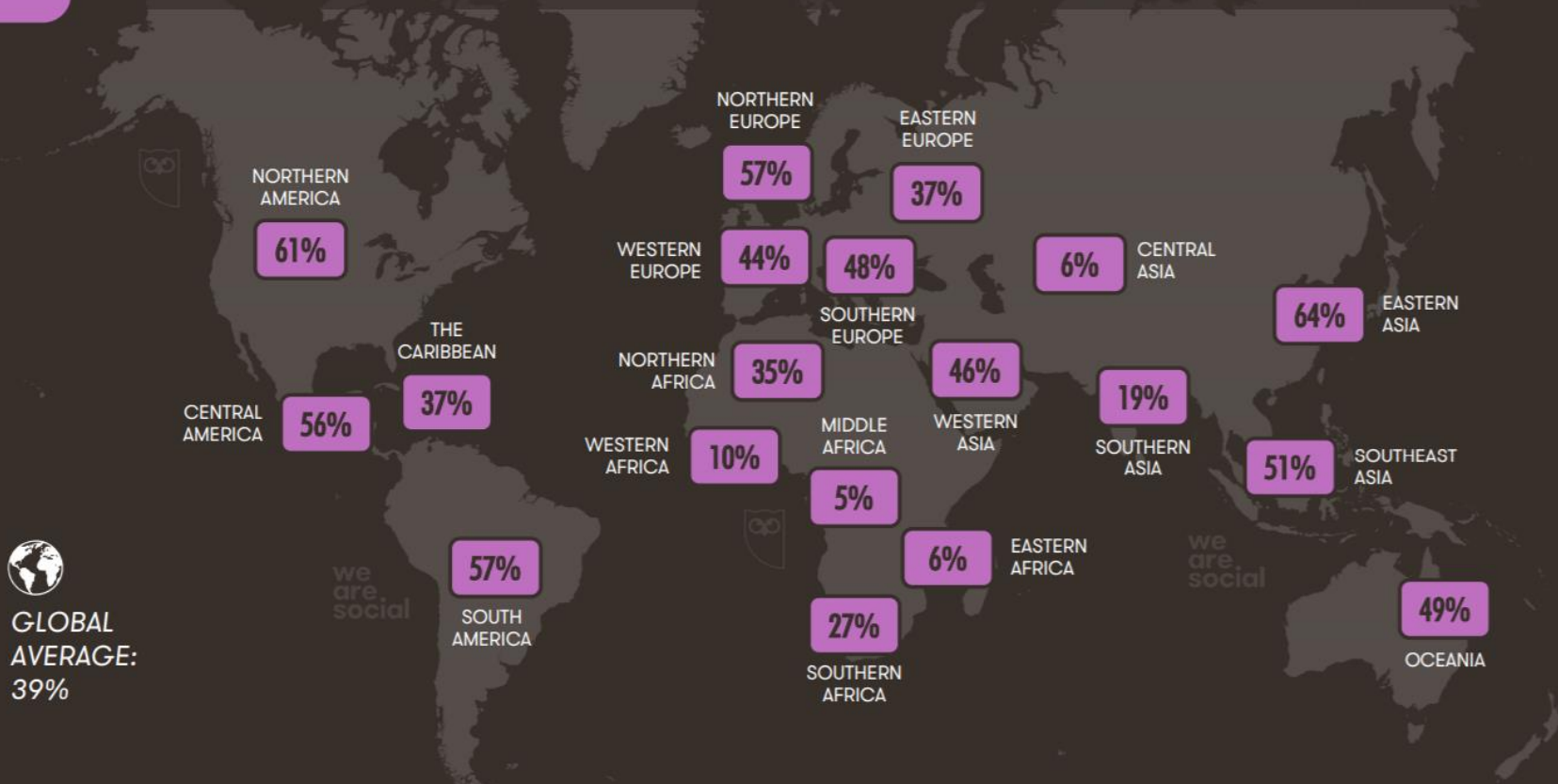
MESSENGER / CHAT APP / VOIP



JAN
2018

MOBILE SOCIAL MEDIA PENETRATION BY REGION

ACTIVE ACCOUNTS ON THE TOP SOCIAL NETWORK IN EACH COUNTRY ACCESSING VIA MOBILE, COMPARED TO POPULATION



JAN
2018

TOP MOBILE APP RANKINGS

RANKINGS OF TOP MOBILE APPS BY MONTHLY ACTIVE USERS AND BY NUMBER OF DOWNLOADS

RANKING OF MOBILE APPS BY MONTHLY ACTIVE USERS

#	APP NAME	DEVELOPER / COMPANY
01	FACEBOOK	FACEBOOK
02	WHATSAPP MESSENGER	FACEBOOK
03	WECHAT	<i>App Annie</i> TENCENT
04	FACEBOOK MESSENGER	FACEBOOK
05	QQ	TENCENT
06	INSTAGRAM	<i>we are social</i> FACEBOOK
07	TAOBAO	ALIBABA GROUP
08	ALIPAY	ANT FINANCIAL SERVICES GROUP
09	WIFI MASTER KEY	SHANGHAI LANTERN NETWORK
10	TENCENT VIDEO	TENCENT

RANKING OF MOBILE APPS BY NUMBER OF DOWNLOADS

#	APP NAME	DEVELOPER / COMPANY
01	FACEBOOK MESSENGER	FACEBOOK
02	FACEBOOK	FACEBOOK
03	WHATSAPP MESSENGER	FACEBOOK
04	INSTAGRAM	 FACEBOOK
05	SNAPCHAT	SNAP
06	UC BROWSER	ALIBABA GROUP
07	SHAREIT	SHAREIT
08	UBER	<i>App Annie</i> UBER TECHNOLOGIES
09	YOUTUBE	GOOGLE
10	IMO	IMO.IM

SOURCE: APP ANNIE, JANUARY 2018, BASED ON DATA IN THE APP ANNIE 2017 RETROSPECTIVE REPORT. FOR MORE DETAILS, VISIT [HTTPS://WWW.APPANNIE.COM/](https://www.appannie.com/)

NOTES: RANKINGS ARE BASED ON COMBINED DATA FOR BOTH THE APPLE IOS APP STORE AND THE GOOGLE PLAY APP STORE. MONTHLY ACTIVE USER RANKINGS ARE BASED ON MONTHLY AVERAGES FOR FULL-YEAR 2017. **NOTE:** RANKINGS EXCLUDE PRE-INSTALLED APPS, SUCH AS YOUTUBE ON ANDROID DEVICES, AND SAFARI ON APPLE DEVICES.



<https://www.juancmejia.com/wp-content/uploads/2014/02/Estudio-de-estad%C3%ADsticas-de-Internet-y-Redes-Sociales-WeAreSocial-y-Hootsuite.pdf>

**JAN
2018**

SHARE OF FACEBOOK ACCESS

BASED ON EACH OPERATING SYSTEM'S SHARE OF GLOBAL FACEBOOK USERS ACCESSING VIA SMARTPHONES AND / OR TABLETS

PERCENTAGE OF MOBILE
FACEBOOK USERS ACCESSING
VIA ANDROID DEVICES



76.2%

PERCENTAGE OF MOBILE
FACEBOOK USERS ACCESSING
VIA APPLE IOS DEVICES



15.5%

PERCENTAGE OF MOBILE
FACEBOOK USERS ACCESSING VIA
OTHER MOBILE OPERATING SYSTEMS



8.3%

we
are
social



**JAN
2018**












HASHTAG AND EMOJI RANKINGS

BASED ON THE NUMBER OF TIMES PEOPLE USED EACH HASHTAG ON INSTAGRAM IN 2017, AND CUMULATIVE EMOJI USE ON TWITTER SINCE JULY 2013

MOST-USED HASHTAGS ON INSTAGRAM IN 2017

#	TOP INSTAGRAM HASHTAGS
01	#LOVE
02	#INSTAGOOD
03	#FASHION
04	#PHOTOOFTHEDAY
05	#BEAUTIFUL
06	#PICOFTHE DAY
07	#FITNESS
08	#STYLE
09	#TRAVEL
10	#HAPPY

MOST-USED EMOJI ON TWITTER (CUMULATIVE)

#	EMOJI	USES ON TWITTER
01		1,955,000,000
02	 	918,000,000
03		727,000,000
04		688,000,000
05		665,000,000
06		556,000,000
07		510,000,000
08		454,000,000
09		402,000,000
10		395,000,000

MOST-USED EMOJI ON TWITTER (CUMULATIVE)

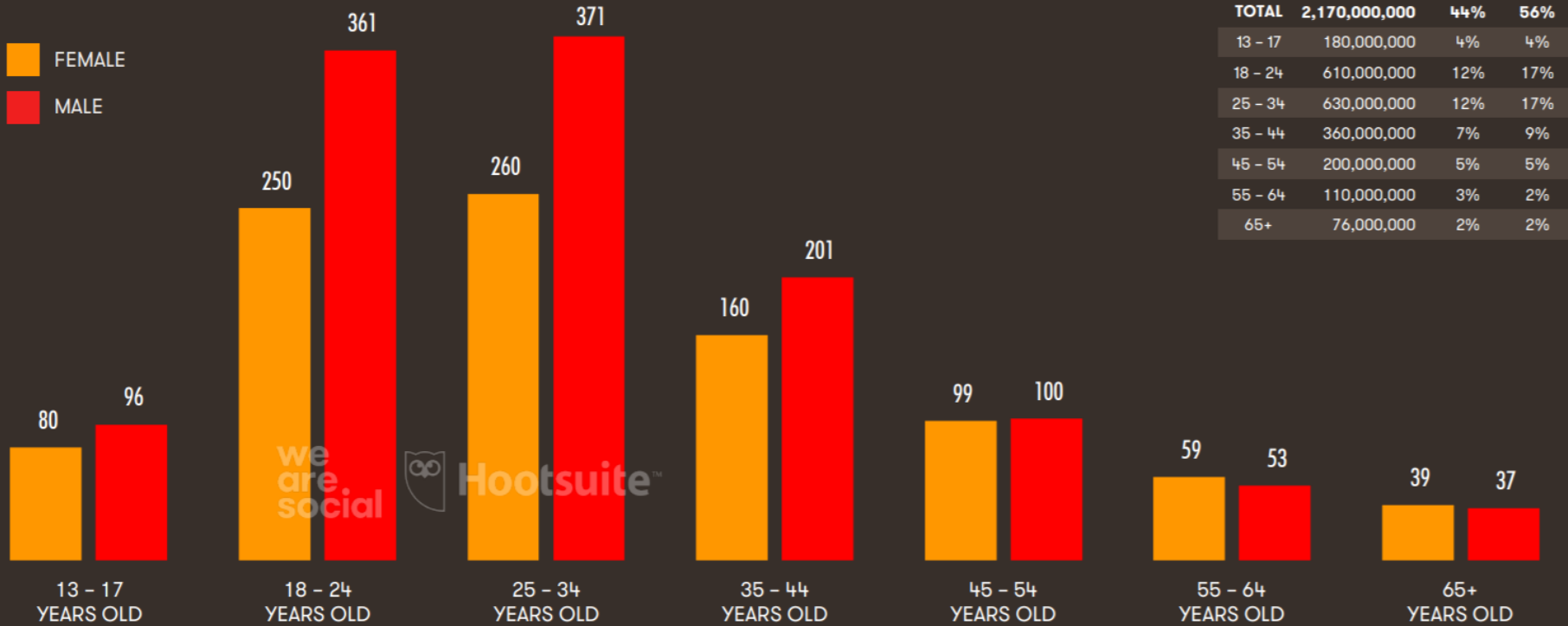
#	EMOJI	USES ON TWITTER
11		359,000,000
12		344,000,000
13		320,000,000
14		295,000,000
15	 	287,000,000
16		282,000,000
17		228,000,000
18		226,000,000
19		198,000,000
20		190,000,000

we
are
social

**JAN
2018**

PROFILE OF FACEBOOK USERS

BREAKDOWN OF FACEBOOK'S GLOBAL USERS BY AGE AND GENDER, IN MILLIONS



SOURCES: EXTRAPOLATION OF FACEBOOK DATA, JANUARY 2018. **NOTES:** THE 'TOTAL' COLUMN OF THE INSET TABLE SHOWS ORIGINAL VALUES, WHILE GRAPH VALUES HAVE BEEN DIVIDED BY ONE MILLION. TABLE PERCENTAGES REPRESENT THE RESPECTIVE GENDER AND AGE GROUP'S SHARE OF TOTAL GLOBAL FACEBOOK USERS. TABLE VALUES MAY NOT SUM EXACTLY DUE TO ROUNDING IN THE SOURCE DATA.

**JAN
2018**

PROFILE OF INSTAGRAM USERS

BREAKDOWN OF INSTAGRAM'S GLOBAL USERS BY AGE AND GENDER, IN MILLIONS



SOURCES: EXTRAPOLATION OF DATA FROM INSTAGRAM (VIA FACEBOOK), JANUARY 2018. **NOTES:** THE 'TOTAL' COLUMN OF THE INSET TABLE SHOWS ORIGINAL VALUES, WHILE GRAPH VALUES HAVE BEEN DIVIDED BY ONE MILLION. TABLE PERCENTAGES REPRESENT THE RESPECTIVE GENDER AND AGE GROUP'S SHARE OF TOTAL GLOBAL INSTAGRAM USERS. TABLE VALUES MAY NOT SUM EXACTLY DUE TO ROUNDING IN THE SOURCE DATA.

**JAN
2018**

INSTAGRAM'S TOP COUNTRIES

COUNTRIES WITH THE LARGEST ACTIVE INSTAGRAM USER BASES, BY TOTAL NUMBER OF USERS AND BY PENETRATION

COUNTRIES WITH THE LARGEST NUMBER OF ACTIVE INSTAGRAM USERS

#	COUNTRY	USERS	PENETRATION
01	UNITED STATES	110,000,000	34%
02	BRAZIL	57,000,000	27%
03	INDONESIA	53,000,000	20%
04	INDIA	52,000,000	4%
05	TURKEY	33,000,000	41%
06	RUSSIA	29,000,000	20%
07	IRAN	24,000,000	29%
08	JAPAN	22,000,000	17%
09	UNITED KINGDOM	21,000,000	32%
10	MEXICO	20,000,000	15%

COUNTRIES WITH THE HIGHEST INSTAGRAM PENETRATION RATES

#	COUNTRY	PENETRATION	USERS
01	BRUNEI DARUSSALAM	49%	210,000
02	SWEDEN	47%	4,700,000
03	ARUBA	46%	49,000
04	CAYMAN ISLANDS	45%	28,000
05	ICELAND	45%	150,000
06	NORWAY	43%	2,300,000
07	BAHRAIN	43%	660,000
08	CYPRUS	42%	500,000
09	TURKEY	41%	33,000,000
10	ISRAEL	39%	3,300,000



we
are
social

2. Modelo de negocio

Facebook fue diseñada para crear adicción

Exempleados de Google y Facebook se organizan para forzar cambios que frenen los excesos de las grandes compañías del sector

https://elpais.com/tecnologia/2018/07/26/actualidad/1532614407_402741.html

- **Diseñadas para crear adicción**
 - Plataformas y servicios sin apenas regulación
 - Carencia de elementos éticos en el diseño
 - En 2017, Facebook ya conocía las evidencias del mal uso de su plataforma mediante cuentas falsas creadas por piratas informáticos rusos para amplificar noticias falsas.
 - Zuckerberg consideró que Facebook no era un medio de comunicación ni era responsable de las acciones de terceros.
- **Instrumentalizada con fines contrarios a la salud**
 - Los algoritmos enfatizan los mensajes negativos:
 - Inducción a la anorexia, miedo, odio... enganchan mejor.

Exempleados de Google y Facebook se organizan para forzar cambios que frenen los excesos de las grandes compañías del sector

https://elpais.com/tecnologia/2018/07/26/actualidad/1532614407_402741.html

- **Modelo de negocio: incremento constante del número de usuarios y de sus interacciones**
 - **Objetivo: aumentar su base de datos de usuarios, y con ella los ingresos por publicidad.**
 - Ofertada como un producto (y no un servicio) reduciría su margen de negocio.
 - El departamento de publicidad tenía **pocos recursos para asegurar que no se vulneraba el derecho a la privacidad.**
 - Criterio corporativo: hacer lo posible por incrementar el número de usuarios conectados y sus interacciones, focalizando la atención con todos los medios posibles.

Una característica del servicio, no un *bug*

N. Carr (19/08/2018): <https://www.wired.com/story/its-not-a-bug-its-a-feature>

- **Carr: *It's not a bug, it's a feature* (INABIAF)**
 - Una excusa para programadores, o algo sobre lo que hackers externos pueden discrepar.
 - **Apunta a un problema de transparencia en el diseño de algoritmos**
 - **En el caso de Facebook, las herramientas centrales habían sido diseñadas para facilitar la venta de datos a otras compañías de publicidad o similares.**

“A standard joke is that a bug can be turned into a feature simply by documenting it (then theoretically no one can complain about it because it's in the manual), or even by simply declaring it to be good. “That's not a bug, that's a feature!” is a common catchphrase.”

The Jargon File, a lexicon of hacker-speak (Stanford, 1975; MIT)

Kwon, S. J., Park, E., & Kim, K. J. (2014). What drives successful social networking services? A comparative analysis of user acceptance of Facebook and Twitter.

The Social Science Journal, 51(4), 534–544. <https://doi.org/10.1016/j.soscij.2014.04.005>

- **Percibida como la plataforma más segura**
 - **Da a los usuarios más elementos de control** sobre niveles de acceso a su información para otros contactos.
 - Pero ha estado **involucrada en múltiples incidentes, brechas de seguridad y malas prácticas**:
 - Podía **manipular feeds** y reorientar la atención a gran escala
 - Ha colaborado en campañas de **vigilancia** sobre los contenidos que actualizaban sus usuarios, **permitiendo acceso a terceros**.
 - Ha sido **instrumentalizada a gran escala** con **actores que podían generar múltiples perfiles falsos y amplificar mensajes** con fines de intoxicación o distorsión política.
 - Menor confianza que Twitter e Instagram en lo sucesivo.

Shane-Simpson, C. et al. (2018). Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Computers in Human Behavior*, 86, 276–288. [10.1016/j.chb.2018.04.041](https://doi.org/10.1016/j.chb.2018.04.041)

- **Competencia Facebook - Instagram**

- Instagram ofrece muchas oportunidades de interactuar con grandes audiencias a través de imágenes autopromocionales
 - Compite con Facebook (2,000 mill. Usuarios, dic. 2017) por atraer a las personas con más rasgos narcisistas.
 - Instagram (1,000 mill., jun. 2018) ha consolidado el fenómeno de los micro-influencers (usuarios de medios sociales con muchos seguidores activos) y es vista como **la mejor plataforma de medios sociales para atraer audiencias** (K. [Morrison](#), 2016).
 - Facebook ha potenciado la gestión de imágenes y vídeo para retener audiencia y círculos de afinidad social, en parte a la zaga del éxito de Instagram para generar sentimientos de intimidad y conexión.
 - **Atracción/retención de audiencia femenina**, con **preferencias de privacidad mejor alineadas con el perfil de intimidad deseado para sus imágenes**.
 - Esta conducta se extiende a Facebook, Pinterest e Instagram.

Cómo gestionar la privacidad de más de 2,000 millones de usuarios

Dhillon, G., Oliveira, T., & Syed, R. (2018). Value-based information privacy objectives for Internet Commerce. *Computers in Human Behavior*, 87, 292–307. doi: [10.1016/j.chb.2018.05.043](https://doi.org/10.1016/j.chb.2018.05.043)

• **Publicidad segmentada según perfiles**

- Elementos superficiales permiten filtrar por categorías (zonas urbanas, áreas, género, uso personal o profesional...
 - No se requiere una violación estricta de la privacidad: basta una gestión eficiente de tendencias de uso, redes de likes, nodos más activos, usuarios con medio de pago, metaetiquetas y detalles mediante **análisis de imágenes por AI y control de feeds**

→ Por eso **Facebook adquirió Instagram (\$1.000 mill. en abril 2012).**

– **Reajuste según tendencias observadas en Instagram**

- De los grandes bloggers (celebridades) a micro-influenciadores/impulsores de tendencia: "**influencers de tamaño medio, con seguidores dedicados y altamente comprometidos**".
- Casi el 60% de 2.500 micro-influencers consideraban Instagram más efectivo para atraer audiencia, frente a 18% de Facebook (Bloglovin)
- Movilidad, seguridad, flexibilidad y calidad del servicio explicaban hace pocos años la disposición a usar Facebook. Pero la **tendencia comercial de Instagram triunfó**.
 - Kwon, S. J. et al. (2014). What drives successful social networking services? A comparative analysis of user acceptance of Facebook and Twitter. *The Social Science Journal*, 51(4), 534–544. <https://doi.org/10.1016/j.soscij.2014.04.005>

3. Acceso privilegiado a terceros

Cambridge Analytica no aprovechó una brecha de seguridad: explotó características del servicio

Numerosas brechas de seguridad

Guardian

The
Guardian

News Opinion Sport Culture Lifestyle



The breach was discovered by Facebook engineers on Tuesday 25 September, the company said, and patched on Thursday.

Facebook says nearly 50m users
compromised in huge security breach



According to Facebook, the attacker exploited three bugs that were introduced into the site's "view as" feature in July 2017. "View as" allows users to see what their profile looks like to other users.

25/09/2018



Numerosas brechas de seguridad

<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

  The data analytics firm that worked with Donald Trump's election team and the winning Brexit campaign harvested millions of Facebook profiles of US voters, in one of the tech giant's biggest ever data breaches, and used them to build a powerful software program to predict and influence choices at the ballot box.

The data was collected through an app called *thisisyourdigitallife*, built by academic Aleksandr Kogan, separately from his work at Cambridge University. Through his company Global Science Research (GSR), in collaboration with Cambridge Analytica, hundreds of thousands of users were paid to take a personality test and agreed to have their data collected for academic use.

obtain the data, told the *Observer*: “We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on.”

Numerosas brechas de seguridad

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in maior data breach

The International edi

Wylie, a Canadian data analytics expert who worked with Cambridge Analytica and Kogan to devise and implement the scheme, showed a dossier of evidence about the data misuse to the *Observer* which appears to raise

'I made Steve Bannon's psychological warfare tool': meet the

questions about their testimony. He has passed it to the National Crime Agency's cybercrime unit and the Information Commissioner's Office. It includes emails, invoices, contracts and bank transfers that reveal more than 50 million profiles - mostly belonging to registered US voters - were harvested from the site in one of the largest-ever breaches of Facebook data.



4. ¿Alternativas?

Las plataformas de interacción social pueden incentivar mejor la privacidad y la seguridad

Incorporar herramientas adecuadas al perfil de usuarios

Wang, H., He, D., & Yu, J. (2019). Privacy-preserving incentive and rewarding scheme for crowd computing in social media. *Information Sciences*, 470, 15–27. doi: [10.1016/j.ins.2018.07.016](https://doi.org/10.1016/j.ins.2018.07.016)

- **Los usuarios eligen sus plataformas de interacción social según intereses específicos**
 - En Twitter optan más por perfiles públicos que privados, porque el objetivo es compartir y acceder a información.
 - En Facebook se prefiere conectar con amigos conocidos en persona, en contextos/actividades offline.
 - Perciben Facebook más seguro que Twitter, por sus opciones de privacidad.
 - En Instagram prevalecen las interacciones recíprocas, con audiencias más amplias que en Facebook
 - Herramienta ideal para perfiles narcisistas (Panek, 2013. [doi: 10.1016/j.chb.2013.04.012](https://doi.org/10.1016/j.chb.2013.04.012))
 - Según fines y características de los usuarios, el diseño de las plataformas puede incluir herramientas adecuadas para incentivar prácticas que garanticen la identidad, eviten fugas de datos y usos o accesos indebidos.

Funcionalidad y control supeditados al servicio

Wang, H., He, D., & Yu, J. (2019). Privacy-preserving incentive and rewarding scheme for crowd computing in social media. *Information Sciences*, 470, 15–27. doi: [10.1016/j.ins.2018.07.016](https://doi.org/10.1016/j.ins.2018.07.016)

- **Los usuarios explotan las debilidades de ciertos servicios para saltarse las reglas**
 - Facebook es el **lugar preferido para compartir contenidos de connotaciones sociales negativas**.
 - La **capacidad de supervisión es limitada en todas las plataformas**; pero da resultados distintos según el tipo de contenidos que predomina en cada una: Twitter: texto breve; Instagram: intercambio de imágenes visuales;
 - **Facebook**: texto, fotos compartidas y diversas opciones de privacidad que permiten establecer quién puede acceder a cada mensaje.
 - **Complejidad técnica y alto coste en recursos humanos de las funciones de curaduría/supervisión de contenidos** disponibles en Facebook: es el **canal idóneo para compartir emociones negativas por la sofisticación de las opciones de privacidad que ofrece**.

Conclusiones

- **Riesgos de ceder a empresas y algoritmos sustitativos del criterio humano la gestión de la interacción social virtual...**
 - En plataformas y servicios diseñados solo bajo criterios de rentabilidad comercial, con funciones que los usuarios ignoran mientras las usan.
 - Impulsados por millones de usuarios a una posición de cuasi monopolio
 - Bajo una dinámica orientada más a la expansión del servicio y aumento de usuarios que a garantizar la calidad, privacidad y fiabilidad del mismo.
 - Con numerosos incidentes y brechas de seguridad de los que no rinden cuentas ante ningún regulador
 - Sin mecanismos de transparencia, auditabilidad y capacidad técnica para supervisar su captura por actores con fines delictivos.
 - Con capacidad para manipular el sistema de feeds y sus objetivos.
 - Dando acceso a terceros, con diversos métodos, para fines comerciales (sin limitarse a la propaganda política del mejor postor).
 - **Debates pendientes** en sociedades hiperconectadas.

Referencias y bibliografía

- De Salve, A., Mori, P., & Ricci, L. (2018). A survey on privacy in decentralized online social networks. *Computer Science Review*, 27, 154–176. <https://doi.org/https://doi.org/10.1016/j.cosrev.2018.01.001>
- Dhillon, G., Oliveira, T., & Syed, R. (2018). Value-based information privacy objectives for Internet Commerce. *Computers in Human Behavior*, 87, 292–307. <https://doi.org/https://doi.org/10.1016/j.chb.2018.05.043>
- Economist, T. (2018). What to make of Mark Zuckerberg's testimony. Retrieved April 15, 2018, from <https://www.economist.com/news/leaders/21740401-both-facebook-boss-and-his-questioners-congress-fail-reassure-what-make-mark>
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. <https://doi.org/10.1016/j.cose.2015.07.002>
- Korea, S., & Ten, F. (2017). The world's most valuable resource: Data and the new rules. *The Economist*, 9, 19–22.
- Marzbali, M. A., Delavari, A., & Souril, F. (2016). Agent, Structure, and the Media-based Democratic Politics. *Procedia - Social and Behavioral Sciences*, 217, 1225–1232. <https://doi.org/https://doi.org/10.1016/j.sbspro.2016.02.154>
- M-Bascuñán, M. (2018). Controladores sin control. Retrieved April 7, 2018, from https://elpais.com/elpais/2018/04/06/opinion/1523014815_288419.html
- Nam, T. (2017). A tool for liberty or oppression? A cross-national study of the Internet's influence on democracy. *Telematics and Informatics*, 34(5), 538–549. <https://doi.org/10.1016/j.tele.2016.11.004>
- Panek, E. T., Nardis, Y., & Konrath, S. (2013). Mirror or Megaphone?: How relationships between narcissism and social networking site use differ on Facebook and Twitter. *Computers in Human Behavior*, 29(5), 2004–2012. <https://doi.org/10.1016/j.chb.2013.04.012>
- Teles, A. S., Silva e Silva, F. J. da, & Endler, M. (2017). Situation-based privacy autonomous management for mobile social networks. *Computer Communications*, 107, 75–92. <https://doi.org/https://doi.org/10.1016/j.comcom.2017.04.003>
- Wei, Z., Wu, Y., Yang, Y., Yan, Z., Pei, Q., Xie, Y., & Weng, J. (2018). AutoPrivacy: automatic privacy protection and tagging suggestion for mobile social photo. *Computers & Security*. <https://doi.org/https://doi.org/10.1016/j.cose.2017.12.002>
- Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies*, 98, 95–108. <https://doi.org/10.1016/j.ijhcs.2016.09.006>

Referencias y bibliografía

- Bioglio, L., & Pensa, R. G. (2017). Impact of Neighbors on the Privacy of Individuals in Online Social Networks. *Procedia Computer Science*, 108, 28–37. <https://doi.org/https://doi.org/10.1016/j.procs.2017.05.030>
- Choi, H. S., Lee, W. S., & Sohn, S. Y. (2017). Analyzing research trends in personal information privacy using topic modeling. *Computers & Security*, 67, 244–253. <https://doi.org/https://doi.org/10.1016/j.cose.2017.03.007>
- Coelho, J., Rito, F., & Duarte, C. (2017). “You, me & TV” — Fighting social isolation of older adults with Facebook, TV and multimodality. *International Journal of Human-Computer Studies*, 98, 38–50. <https://doi.org/https://doi.org/10.1016/j.ijhcs.2016.09.015>
- DasGupta, B., Mobasher, N., & Yero, I. G. (2019). On analyzing and evaluating privacy measures for social networks under active attack. *Information Sciences*, 473, 87–100. <https://doi.org/https://doi.org/10.1016/j.ins.2018.09.023>
- Dhir, A., Khalil, A., Lonka, K., & Tsai, C.-C. (2017). Do educational affordances and gratifications drive intensive Facebook use among adolescents? *Computers in Human Behavior*, 68, 40–50. <https://doi.org/https://doi.org/10.1016/j.chb.2016.11.014>
- James, T. L., Wallace, L., Warkentin, M., Kim, B. C., & Collignon, S. E. (2017). Exposing others’ information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use. *Information & Management*, 54(7), 851–865. <https://doi.org/https://doi.org/10.1016/j.im.2017.01.001>
- Jeong, Y., & Kim, Y. (2017). Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. *Computers in Human Behavior*, 69, 302–310. <https://doi.org/https://doi.org/10.1016/j.chb.2016.12.042>
- Pardo, R., Balliu, M., & Schneider, G. (2017). Formalising privacy policies in social networks. *Journal of Logical and Algebraic Methods in Programming*. <https://doi.org/10.1016/j.jlamp.2017.02.008>
- Pensa, R. G., & Di Blasi, G. (2017). A privacy self-assessment framework for online social networks. *Expert Systems with Applications*, 86, 18–31. <https://doi.org/https://doi.org/10.1016/j.eswa.2017.05.054>
- Romero, P. (2018). En Facebook no eres usuario , eres producto. Retrieved April 7, 2018, from <http://www.publico.es/sociedad/proteccion-datos-facebook-no-usuario-producto.html>
- Sahinoglu, M., Akkaya, A. D., & Ang, D. (2012). Can We Assess and Monitor Privacy and Security Risk for Social Networks? *Procedia - Social and Behavioral Sciences*, 57, 163–169. <https://doi.org/https://doi.org/10.1016/j.sbspro.2012.09.1170>
- van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, 78, 283–297. <https://doi.org/https://doi.org/10.1016/j.chb.2017.10.007>

Referencias y bibliografía

- Al Swelmiyeen, I., & Al-Nuemat, A. (2017). Facebook e-court: Online justice for online disputes. *Computer Law & Security Review*, 33(2), 223–236. <https://doi.org/https://doi.org/10.1016/j.clsr.2016.11.006>
- Chang, S. E., Liu, A. Y., & Shen, W. C. (2017). User trust in social networking services: A comparison of Facebook and LinkedIn. *Computers in Human Behavior*, 69, 207–217. <https://doi.org/https://doi.org/10.1016/j.chb.2016.12.013>
- Crabtree, M. A., & Pillow, D. R. (2017). Extending the Dual Factor Model of Facebook Use: Social motives and network density predict Facebook use through impression management and open self-disclosure. *Personality and Individual Differences*. <https://doi.org/https://doi.org/10.1016/j.paid.2017.06.017>
- Kwon, S. J., Park, E., & Kim, K. J. (2014). What drives successful social networking services? A comparative analysis of user acceptance of Facebook and Twitter. *The Social Science Journal*, 51(4), 534–544. <https://doi.org/10.1016/j.soscij.2014.04.005>
- Lankton, N. K., McKnight, D. H., & Tripp, J. F. (2017). Facebook privacy management strategies: A cluster analysis of user privacy behaviors. *Computers in Human Behavior*, 76, 149–163. <https://doi.org/https://doi.org/10.1016/j.chb.2017.07.015>
- Leiner, D. J., Kobilke, L., Rueß, C., & Brosius, H.-B. (2018). Functional domains of social media platforms: Structuring the uses of Facebook to better understand its gratifications. *Computers in Human Behavior*, 83, 194–203. <https://doi.org/https://doi.org/10.1016/j.chb.2018.01.042>
- Morozov, E. (2018). After the Facebook scandal it's time to base the digital economy on public v private ownership of data | Technology | The Guardian. Retrieved July 17, 2018, from <https://www.theguardian.com/technology/2018/mar/31/big-data-lie-exposed-simply-blaming-facebook-wont-fix-reclaim-private-information>
- Oeldorf-Hirsch, A., Birnholtz, J., & Hancock, J. T. (2017). Your post is embarrassing me: Face threats, identity, and the audience on Facebook. *Computers in Human Behavior*, 73, 92–99. <https://doi.org/https://doi.org/10.1016/j.chb.2017.03.030>
- Panek, E. T., Nardis, Y., & Konrath, S. (2013). Mirror or Megaphone?: How relationships between narcissism and social networking site use differ on Facebook and Twitter. *Computers in Human Behavior*, 29(5), 2004–2012. <https://doi.org/10.1016/j.chb.2013.04.012>
- Tsai, T.-H., Chang, H.-T., Chang, Y.-C., & Chang, Y.-S. (2017). Personality disclosure on social network sites: An empirical examination of differences in Facebook usage behavior, profile contents and privacy settings. *Computers in Human Behavior*, 76, 469–482. <https://doi.org/https://doi.org/10.1016/j.chb.2017.08.003>

Referencias y bibliografía

- Brown, G., Michinov, N., & Manago, A. M. (2017). Private message me s'il vous plait: Preferences for personal and masspersonal communications on Facebook among American and French students. *Computers in Human Behavior*, 70, 143–152. <https://doi.org/https://doi.org/10.1016/j.chb.2016.12.051>
- Casale, S., & Fioravanti, G. (2018). Why narcissists are at risk for developing Facebook addiction: The need to be admired and the need to belong. *Addictive Behaviors*, 76, 312–318. <https://doi.org/https://doi.org/10.1016/j.addbeh.2017.08.038>
- Jung, E. H., Walden, J., Johnson, A. C., & Sundar, S. S. (2017). Social networking in the aging context: Why older adults use or avoid Facebook. *Telematics and Informatics*, 34(7), 1071–1080. <https://doi.org/https://doi.org/10.1016/j.tele.2017.04.015>
- Leong, L.-Y., Jaafar, N. I., & Ainin, S. (2018). The effects of Facebook browsing and usage intensity on impulse purchase in f-commerce. *Computers in Human Behavior*, 78, 160–173. <https://doi.org/https://doi.org/10.1016/j.chb.2017.09.033>
- Lev-On, A. (2017). The third-person effect on Facebook: The significance of perceived proficiency. *Telematics and Informatics*, 34(4), 252–260. <https://doi.org/https://doi.org/10.1016/j.tele.2016.07.002>
- Shiau, W.-L., Dwivedi, Y. K., & Lai, H.-H. (2018). Examining the core knowledge on facebook. *International Journal of Information Management*, 43, 52–63. <https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2018.06.006>
- Su, C. C., & Chan, N. K. (2017). Predicting social capital on Facebook: The implications of use intensity, perceived content desirability, and Facebook-enabled communication practices. *Computers in Human Behavior*, 72, 259–268. <https://doi.org/https://doi.org/10.1016/j.chb.2017.02.058>
- Symeonidis, I., Biczók, G., Shirazi, F., Pérez-Solà, C., Schroers, J., & Preneel, B. (2018). Collateral damage of Facebook third-party applications: a comprehensive study. *Computers & Security*, 77, 179–208. <https://doi.org/https://doi.org/10.1016/j.cose.2018.03.015>
- Wang, R., & Yu, N. (2018). Friending instructors on Facebook: Exploring the role of privacy on student-instructor connection on cyberspace. *Telematics and Informatics*. <https://doi.org/https://doi.org/10.1016/j.tele.2018.02.004>
- Zarouali, B., Ponnet, K., Walrave, M., & Poels, K. (2017). “Do you like cookies?” Adolescents’ skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing. *Computers in Human Behavior*, 69, 157–165. <https://doi.org/https://doi.org/10.1016/j.chb.2016.11.050>