ISSN (electrónico): 2014-2242 / www.cac.cat

QUADERNS DEL CAC

Tus *likes* ¿tu voto? Explotación masiva de datos personales y manipulación informativa en la campaña electoral de Donald Trump a la presidencia de EEUU 2016

Sara Suárez-Gonzalo

Investigadora predoctoral del Departament de Comunicació de la Universitat Pompeu Fabra

sarapaz.suarez@upf.edu

Código ORCID: orcid.org/0000-0001-6883-1984.

Artículo recibido el 23/04/2018 y aceptado el 11/07/2018

Resumen

Los diarios Observer *y* The New York Times *han revelado un supuesto escándalo de corrupción de datos a escala masiva que involucra a Facebook y a Cambridge Analytica y que podría haber favorecido la victoria electoral de Donald Trump.*

El objetivo de este artículo es analizar las condiciones de posibilidad del caso y de su potencial influencia en la decisión de voto estadounidense. Para ello se examina el contexto científico-tecnológico, empresarial y legal relacionado con las tecnologías big data en el que se habrían producido los hechos, y se valora su posible influencia en relación con las limitaciones propias de la estrategia empleada y su contexto mediático y sociopolítico actual.

Palabras clave

Big data*, protección de datos personales, Donald Trump, Facebook, Cambridge Analytica, manipulación informativa.*

Abstract

The newspapers Observer *and* The New York Times *have revealed an alleged massive-scale scandal of data corruption involving Facebook and Cambridge Analytica that could have benefited the electoral victory of Donald Trump.*

The objective of this article is to analyze the conditions of possibility of the case and its potential influence on Americans' voting decision. To do so, it examines the scientific-technological, business and legal context related to big data technologies in which the facts would have happened and evaluates their possible influence in relation to the limits of the performed strategy and its current media and socio-political context.

Keywords

Big data, personal data protection, Donald Trump, Facebook, Cambridge Analytica, media manipulation.

Introducción

El 17 de marzo de 2018, los diarios *Observer* y *The New York Times* publicaron el testimonio de un nuevo "soplón" llamado Christopher Wylie. Las noticias revelan un supuesto traspaso indebido de los datos de millones de usuarios de Facebook a la empresa Cambridge Analytica, que esta habría utilizado para favorecer la victoria de Donald Trump en las elecciones generales estadounidenses de 2016 mediante una estrategia de *microtargeting* basada en técnicas militares de ataque psicológico. También se ha expuesto que una parte de los datos, recogidos en el Reino Unido, podrían haber sido utilizados en las campañas "Vote Leave" y "BeLeave" para favorecer el sí al *Brexit* en el referéndum realizado el 23 de junio de 2016.

Debido en parte a filtraciones tan mediáticas como esta, relacionadas con la corrupción de datos, y las posibilidades que, a día de hoy, proporcionan las tecnologías de recopilación y análisis de datos masivos (*big data*), la preocupación ciudadana por la privacidad de los datos personales ha aumentado en los últimos años (Hargittai y Marwick 2016; Turow, Hennessy y Draper 2015). Pese a que la analítica *big data* no deja de ser una forma de análisis cuantitativo más desarrollada, sí conlleva importantes novedades: la recopilación de datos es indiscriminada y su tratamiento se sirve de técnicas de agregación y cruce de datos (Baruh y Popescu 2015) que permiten inferir información que los datos no contienen de forma explícita (Tufekci 2015). Diferentes disciplinas académicas han contribuido de manera determinante al desarrollo técnico de las posibilidades que ofrece el análisis de datos masivos y al abaratamiento de sus costes. Como resultado, organizaciones e instituciones públicas y privadas ya han comenzado a utilizar los datos masivos para fines diversos. Las predicciones de mercado, la publicidad dirigida, la mejora del sector de transportes, la persecución del terrorismo, la salud pública o la gestión de los desastres naturales son solo algunos ejemplos (Resolución del Parlamento Europeo de 14 de marzo de 2017). Pero más allá de esto, empieza a consolidarse un modelo de negocio basado en la explotación de datos y dominado por las grandes multinacionales tecnológicas.

Las tecnologías *big data*, además de ser cada vez más

complejas, son especialmente opacas (Pasquale 2015), dado que existen grandes intereses de poder en disputa tras la explotación de datos. Por ello, el modelo de la notificación y la elección (*notice and choice*) (Baruh y Popescu 2015) que fundamenta las leyes occidentales de protección de datos resulta insuficiente para hacer frente al impacto social del fenómeno *big data* (Suárez-Gonzalo 2017).

Como todo avance tecnológico, los métodos y las herramientas de recopilación y analítica *big data* corren el peligro de caer en las manos equivocadas, o de ser mal utilizados. El caso Cambridge Analytica representa este peligro, pero más allá de esto, ilustra muchos de los riesgos que conlleva la evolución actual del fenómeno *big data*. Por una parte, pone de manifiesto las amenazas que este supone para la privacidad y la protección de los datos personales, así como las carencias de la legislación actual. Por otra, permite discutir su influencia en el auge de la manipulación informativa, la desinformación en la red o la radicalización de las ideas y las opiniones políticas (Marwick y Lewis 2017).

El objetivo de este artículo es explicar que la gravedad del caso Cambridge Analytica está más relacionada con la existencia de una estructura que lo hace posible y con el impacto social de la misma, y no tanto con la posible interferencia concreta que haya ejercido el caso en la decisión de voto estadounidense. Para dar respuesta a este objetivo, el artículo se divide en dos partes. En primer lugar, presenta una descripción de los hechos revelados por *Observer* y *The New York Times* y analiza su condición de posibilidad en relación con las características del contexto científico-tecnológico, empresarial y legal en el que estos se habrían producido. Cabe destacar que este artículo se centra en la vertiente estadounidense del caso, que ha sido la más notoria y de la que se han confirmado más datos hasta el momento por medio de otras fuentes. Por otra parte, dado que la publicación de la información es todavía muy reciente y que no se trata de hechos probados, cabe recalcar que la argumentación presentada en este estudio no depende de la veracidad o exactitud de los mismos, sino que se fundamenta en un análisis de sus condiciones de posibilidad. Con esto se pretende explicar que el caso, lejos de ser la causa del problema, es su esperable consecuencia. La segunda parte se focaliza en la posible influencia del caso Cambridge Analytica. Siguiendo la misma lógica de la primera parte, en ella se explica cuál es el tipo de influencia que ejerce sobre las personas la técnica del *microtargeting.* Seguidamente, se cuestiona el nivel de esta influencia en la decisión de voto estadounidense, en relación con las limitaciones del modelo utilizado para dibujar el perfil del público objetivo de dicha campaña, por una parte; y por otra, de acuerdo con el contexto mediático y sociopolítico actual en el que se inscribe el caso.

Para dar respuesta a este objetivo, se utilizan tres tipos de fuentes principales: científicas, periodísticas y corporativas. Dada la naturaleza teórica del estudio, la producción científica es la fuente más relevante y la que fundamenta la argumentación desarrollada. En segundo lugar, las fuentes periodísticas sirven para explicar el caso Cambridge Analytica. Tras consultar un amplio corpus de noticias, se seleccionaron las que contenían más información detallada sobre los hechos: dos publicadas por *Observer* el 17 de marzo de 2018 (día en el que se destapó el caso) y una publicada por *The New York Times* (medios que destaparon el caso). A estas tres se suma una cuarta, publicada por *Observer* un año antes de la filtración (7 de mayo de 2017) cuando el diario comenzó a desvelar información relevante, mediante la confesión de un informador aún en la sombra. Por último, se han consultado dos clases de fuentes corporativas: por una parte, las páginas web de las empresas implicadas (Cambridge Analytica y SCL Group), donde estas autodescriben su modelo de negocio; y por otra, comunicados e informes oficiales publicados por Facebook acerca del caso.

Tu vida digital, Cambridge Analytica y la campaña electoral de Trump

Las últimas estimaciones de Facebook (Schroepfer, 4 de abril de 2018) confirman que durante el año 2014 se produjo una filtración de datos de aproximadamente 87 millones de usuarios de Facebook a la empresa Cambridge Analytica. De estos 87, más de 70 millones corresponderían a perfiles de ciudadanos estadounidenses. Más de 1 millón de los restantes serían de ciudadanos del Reino Unido y cerca de 137 mil, de españoles.

La obtención de los datos

Según el testimonio del antiguo empleado de Cambridge Analytica y SCL Group, Christopher Wiley, publicado por *Observer - The Guardian* (Cadwalladr y Graham-Harrison, 17 de marzo de 2018; Cadwalladr, 17 de marzo de 2018) y por *The New York Times* (Rosenberg, Confessore y Cadwalladr, 17 de marzo de 2018), el traspaso de los datos se habría producido gracias a la implicación del profesor e investigador de la Universidad de Cambridge, Aleksandr Kogan. Este habría replicado la aplicación myPersonality (Mi personalidad), desarrollada por sus compañeros del Departamento de Psicología, cuyos resultados fueron difundidos en una publicación académica en 2012 (Stillwell y Kosinski 2012). La réplica sería This is Your Digital Life (Esta es tu vida digital), un test de personalidad disponible en Facebook desde 2014 que requería a sus participantes tener una cuenta en Facebook y ser votantes en Estados Unidos. Al participar, los usuarios consentían ceder los datos de su cuenta para fines de investigación académica y a cambio recibían una compensación económica. Según los datos que ha hecho públicos Zuckerberg (21 de marzo de 2018), cerca de 300.000 personas realizaron el test. Pero This is Your Digital Life también dio acceso a Kogan a ciertos datos de los "amigos" de la mayoría de los usuarios participantes en el test, de modo que la cantidad de perfiles de usuario de los que obtuvo datos se incrementó exponencialmente hasta los 87 millones. Debido a que estos "amigos" no habían consentido el acceso a sus perfiles, los datos que se obtuvieron de ellos

fueron fundamentalmente aquellos generados por la propia participación en la red social y que habitualmente son "públicos por defecto".

Según Wiley (Cadwalladr y Graham-Harrison, 17 de marzo de 2018), Kogan habría filtrado estos datos a Cambridge Analytica en 2015, mediante un acuerdo comercial entre su compañía Global Science Research (GSR) y SCL Elections, una sucursal de SCL Group, que es a su vez una compañía afiliada de Cambridge Analytica. Esta filtración no habría sido descubierta hasta aproximadamente un año después, en 2015, por Facebook, quien no puso en conocimiento de los hechos ni a sus usuarios ni a los estados perjudicados.

Los recientes informes y publicaciones oficiales difundidos por las autoridades de Facebook (Grewal, 16 de marzo de 2018; Schroepfer, 4 de abril de 2018; Zuckerberg, 21 de marzo de 2018) confirman el testimonio de Wiley. Ahora, el servicio de ayuda de la red social ha puesto a disposición de los usuarios la herramienta "¿Cómo puedo averiguar si se ha compartido mi información con Cambridge Analytica?" (Facebook 2018), en la que estos pueden comprobar si la empresa de datos ha accedido a información de su perfil.

El análisis de los datos

El método desarrollado por Stillwell y Kosinski (2012), Kosinski, Stillwell y Graepel (2013), y Youyou, Kosinski y Stillwell (2015) para realizar estudios psicométricos a partir de los datos obtenidos mediante myPersonality (Stillwell y Kosinski 2012) le habría servido a Wiley para analizar los datos recogidos mediante la aplicación This is Your Digital Life. Kosinski, Stillwell y Graepel (2013) demostraron la posibilidad de conocer atributos y características personales altamente sensibles a través del análisis automático de registros digitales del comportamiento humano fácilmente accesibles, en este caso, los *likes* ("me gusta") expresados en Facebook. Entre los atributos que el estudio demostró poder predecir se encuentran la orientación sexual, política y religiosa, el sexo, la etnia, o información sobre la trayectoria vital como el consumo de drogas, el nivel de satisfacción con la vida o si los padres de una persona permanecieron juntos hasta que el individuo tenía 21 años. Gracias a ello, Wiley habría obtenido una descripción de los perfiles psicológicos de millones de usuarios involucrados, incluyendo sus afinidades políticas. Los resultados de los tests de personalidad realizados por las casi 300 mil personas que participaron en This is Your Digital Life serían el grupo de control de la validez de los análisis realizados sobre el conjunto completo de los datos.

Según la información publicada por *The Guardian* (Cadwalladr, 7 de mayo de 2017), Cambridge Analytica habría combinado esta información psicológica con información extraída de bases de datos de consumidores y la habría cruzado posteriormente con direcciones postales, correos electrónicos y teléfonos. La propia plataforma Facebook permitía hasta el momento la búsqueda de perfiles a través de números de teléfono o direcciones, opción que, como ha explicado Schroepfer (4 de abril de 2018), ahora la compañía ha desactivado debido a los abusos de actores malintencionados.

La explotación de los datos

El exempleado de Cambridge Analytica ha revelado que estos datos habrían sido utilizados en una campaña de *microtargeting* político con el objetivo de influir en la decisión de voto durante las elecciones presidenciales del 2016 a favor de Donald Trump (Cadwalladr, 17 de marzo de 2018).

Newman (2016) sostiene que la técnica del *microtargeting* ya fue utilizada por los comités de campaña de Obama en las elecciones presidenciales de 2008 y 2012. El *microtargeting* es una técnica de publicidad directa que permite generar campañas más persuasivas al servirse de técnicas de análisis de datos masivos y de mecanismos de inteligencia artificial para obtener información y dirigirse al público de forma personalizada (Alkış y Taşkaya Temizel 2015; Miralles-Pechuán, Ponce y Martínez-Villaseñor 2017; Neumann 2017).

Sin embargo, en el caso de la campaña de Trump, Christopher Wiley (Cadwalladr, 17 de marzo de 2018) apunta al uso de "operaciones psicológicas" (*psychological operations* o PSYOPS), un tipo de técnicas militares de guerra informativa dedicadas a ejercer una influencia de tipo manipulativo y no persuasivo. Las PSYOPS son un tipo de ataque consistente en localizar objetivos especialmente vulnerables al impacto psicológico y lanzar un mensaje capaz de cambiar sus sentimientos para moverlos a una determinada acción que favorezca los intereses nacionales o de las fuerzas aliadas. Las fuerzas de defensa estadounidenses han efectuado estos ataques informativos antes, después o durante el transcurso de guerras o conflictos (United States Air Force 1999). La investigación desempeñada por Briant (2018) argumenta que, a partir del ataque terrorista perpetrado por Al Qaeda el 11 de septiembre de 2001, el gobierno estadounidense apostó por una extensión del uso de las operaciones psicológicas a los sistemas modernos de propaganda interna del país. En su artículo, Briant argumenta que esta transformación se debe en gran medida a la extensión de las tecnologías de la información y de la comunicación, que desafían la influencia del modelo de propaganda tradicionalmente utilizado por el departamento de Asuntos Públicos de EEUU. Sartonen, Simola, Timonen y Lovén (2017), por su parte, subrayan que una de las grandes potencialidades de los perfiles psicológicos dibujados a través del análisis del comportamiento en la red es su capacidad de contribuir a los objetivos de las PSYOPS.

El caso, posible y necesario

Con el objetivo de tener presentes los hechos a los que nos referimos, cabe señalar que, de confirmarse el testimonio de Wiley:

1. Se habría producido una filtración masiva de datos de usuarios de Facebook por medio de un acuerdo comercial

entre el académico de la Universidad de Cambridge Aleksandr Kogan y SCL Group.
2. En total, esta filtración afectaría a los perfiles de aproximadamente 87 millones de usuarios de Facebook.
3. Como consecuencia, se habría incumplido la normativa de Facebook, que obliga a quien recopila los datos a informar a los usuarios sobre la finalidad de su uso y no permite el traspaso de datos a terceros. En el caso de los países europeos afectados, también se habría incumplido el Reglamento General de Protección de Datos (UE) 2016/679, que prohíbe la venta de datos a terceros.
4. Además, se habría violado el acuerdo alcanzado con los usuarios participantes en This is Your Digital Life, que únicamente habrían consentido dar acceso a la información de sus perfiles para un uso académico.
5. Posteriormente, estos datos habrían sido utilizados para manipular la decisión de voto del electorado estadounidense a favor de la candidatura de Donald Trump, mediante una campaña de *microtargeting* basada en técnicas militares de guerra informativa.

Pese a la existencia de informes que confirmarían, al menos parcialmente, el testimonio de Wiley, la argumentación que se desarrolla en este estudio no depende de la veracidad o exactitud de los hechos revelados, sino de la existencia de las investigaciones académicas que los hacen posibles, de un modelo de negocio que los necesita y de un contexto legal incapaz de hacerle frente.

Así, el presente epígrafe explica las características principales de la investigación académica, el modelo de negocio y el contexto legal relacionados con el caso.

La explotación de datos como línea de investigación académica

En primer lugar, las publicaciones académicas mencionadas en el epígrafe anterior y fundamentalmente ligadas a la psicología, la ciencia computacional y la comunicación demuestran:

1. Que el análisis automático de registros digitales fácilmente accesibles sobre el comportamiento de las personas en sus redes sociales permite conocer una gama de características sensibles de su personalidad, incluyendo la afinidad política (Kosinski, Stillwell y Graepel 2013; Stillwell y Kosinski 2012; Youyou, Kosinski y Stillwell 2015).
2. Que, partiendo del perfil psicológico obtenido en el análisis anterior, es posible elaborar estrategias de comunicación personalizada más persuasivas (Alkış y Taşkaya Temizel 2015; Miralles-Pechuán, Ponce y Martínez-Villaseñor 2017; Neumann 2017).
3. Que el perfil psicológico de las personas tiene un gran interés para la aplicación de técnicas militares de manipulación emocional, capaces de modificar los comportamientos de las personas de acuerdo con unos objetivos concretos (Sartonen, Simola, Timonen y Lovén 2017).

Debido al riesgo social que conlleva esta línea de investigación, parece necesario estipular de forma clara cuáles son sus objetivos para el desarrollo social y cuáles son los ámbitos en los que es legítima su ejecución práctica.

La explotación de datos como modelo de negocio

Por otra parte, las empresas involucradas en el caso, Cambridge Analytica y SCL Group, encarnan un modelo de negocio en expansión que cuenta con el respaldo de inversiones millonarias. Este modelo consiste en la elaboración de campañas de comunicación estratégica cuyo objetivo es modificar el comportamiento de segmentos vulnerables de una audiencia objetivo en favor de objetivos concretos.

Cambridge Analytica (2018) es una empresa con sede en Nueva York, Washington y Londres que se fundó en 2013 como una filial de SCL Group. La empresa, cuyo máximo inversor es el billonario estadounidense Robert Mercer, tiene como director general en Estados Unidos a Steve Bannon, ex consejero estratégico de Donald Trump en la Casa Blanca. Cambridge Analytica se presenta bajo el eslogan "Los datos dirigen todas nuestras acciones" (*Data drives all we do*) como una compañía que "utiliza datos para cambiar el comportamiento de la audiencia". La empresa está formada por una división comercial, dedicada a la publicidad y el marketing, y otra política, dedicada a las campañas de comunicación electoral. Los servicios que ofrece, ya sean dirigidos a consumidores o a votantes, son: investigar a la audiencia objetivo para conocerla en profundidad y comprender sus características principales; enriquecer los datos obtenidos e integrarlos en una plataforma centralizada; predecir segmentos de la audiencia propensos a responder favorablemente a los mensajes, y elaborar campañas multicanal diseñadas a medida para captar a segmentos clave de la audiencia e informar de su futuro alcance mediante los datos de rendimiento de la campaña. A las empresas les prometen conocer a cada individuo de su público objetivo, para ayudarlas a conectar con él "a un nivel personal". A sus clientes de la división política, identificar a su electorado objetivo, conocerlo mejor y conseguir más influencia sobre él para moverlo a la acción, a un coste bajo. En otras palabras, su modelo de negocio consiste en la explotación de datos para modificar el comportamiento de un público objetivo.

Por su parte, SCL Group (2018) también pertenece a Robert Mercer y, como se manifiesta en su página web, es una compañía dedicada a desarrollar campañas de comunicación estratégica para gobiernos y organizaciones militares de todo el mundo a partir del análisis de datos. Su objetivo principal es provocar cambios de comportamiento en operaciones de defensa, inteligencia y cambio social.

En cuanto al modelo de negocio, por lo tanto, es preciso asegurar que los intereses privados de las empresas respeten los derechos de los ciudadanos y la organización democrática de la sociedad.

Insuficiencia legal

Por último, de confirmarse el testimonio de Wiley, se habrían producido presuntas ilegalidades relativas a la obtención de los datos. Este apartado muestra que, más allá de penar estas ilegalidades, el marco legal de protección de datos personales es insuficiente para hacer frente a la situación. Las reflexiones son comunes al caso estadounidense y al europeo, que se fundamentan en el mismo modelo de la notificación y el consentimiento individual (Baruh y Popescu 2015). Este requiere que las personas estén bien informadas sobre lo que ocurre con sus datos, ya que, en función de esta información, deben consentir (o no) cederlos.

Accesibilidad de los datos

Dado que el grueso de la información supuestamente utilizada por Cambridge Analytica para generar una estrategia de influencia en el electorado es fácilmente accesible (*likes*), el hecho de que la haya obtenido de manera ilícita no parece demasiado relevante.

A este respecto, parece necesario puntualizar una cuestión: que los datos sean accesibles no quiere decir que sean de carácter público. Las interfaces de las redes sociales son espacios diseñados y gestionados por empresas privadas con intereses comerciales determinados, y por ello no son exactamente equiparables a los tradicionales espacios públicos. Además, el hecho de que algo sea público no significa que pueda ser utilizado por cualquiera, ni para cualquier uso.

Acuerdo inválido

Por otra parte, al mentir sobre la finalidad de los datos (comercial y no académica), se habría producido una ruptura del acuerdo alcanzado entre las partes: el investigador que solicita el consentimiento al usuario para recoger sus datos, y el usuario que lo proporciona. Más allá de esta ruptura del acuerdo, castigada por la propia red social, el caso Cambridge Analytica demuestra que, como se argumenta en un trabajo anterior (Suárez-Gonzalo 2017), el consentimiento individual es un instrumento inválido para proteger los datos personales, por al menos los siguientes motivos:

1. Es un requisito para la participación y el disfrute de productos y servicios. En el caso de This is Your Digital Life, los usuarios debían aceptar tanto las condiciones de uso del navegador de internet como de Facebook y de la propia aplicación. Además, en este caso la cesión de los datos estaba vinculada a una compensación económica.
2. Debido a la capacidad de las tecnologías de análisis de datos masivos para inferir información latente en los datos, los usuarios consienten dar acceso a unos datos determinados de su perfil, pero desconocen qué información sensible se puede obtener a través de su análisis (Tufekci 2015). Esto significa que, aunque las huellas de nuestro comportamiento básico como usuarios de las redes sociales no serían necesariamente consideradas como datos personales, la información que se puede extraer de su análisis puede llegar a ser de un alto carácter sensible.
3. Por otra parte, la información personal que difunde una persona también afecta a los demás, con lo que una persona no tiene por qué conocer (ni haber consentido) la publicación de información que le afecta. En este sentido, el consentimiento individual tiene un impacto social. El caso de This is Your Digital Life ejemplifica esta cuestión en dos sentidos. Por un lado, el hecho de que un grupo de personas haya participado en el test ha podido utilizarse para perjudicar a otros millones de personas, ajenas a la cuestión. Por el otro, que estas personas hayan dado su consentimiento ayuda a conformar un modelo de negocio basado en la explotación de datos personales que afecta al conjunto de la sociedad.
4. A esta complejidad se le suma la opacidad intencionada de las tecnologías *big data* (Pasquale 2015), que hace que sea especialmente complejo para las personas estar bien informadas sobre lo que ocurre con sus datos a la hora de consentir. Esto supone, además, que el acuerdo alcanzado mediante el consentimiento no conlleva negociación, ni se produce entre partes iguales.

Por estos motivos, es difícil considerar que el consentimiento individual sea un mecanismo válido para proteger los datos personales.

La influencia, en su contexto

El epígrafe anterior se ha centrado en las características del contexto en el que se habría producido el caso Cambridge Analytica. Este se centra en el contexto relativo al tipo y al nivel de influencia del caso.

Dada la gravedad de los hechos revelados, no cabe duda de que es necesario un estudio riguroso sobre la veracidad de los hechos y su nivel de influencia en la victoria de Donald Trump. Sin embargo, centrar la atención de manera excesiva en esta cuestión puede resultar fútil. Primero, porque es difícil medir el grado de influencia de un hecho aislado en una decisión compleja. Segundo, porque podría llevar a minimizar la importancia de que exista un modelo empresarial dedicado, precisamente, a buscar esta influencia. Y además, porque si la tecnología *big data* sigue desarrollándose en el sentido actual, su capacidad de influencia puede ser cada vez mayor.

El objetivo de este apartado es explicar la importancia de centrar la atención en el impacto social del sistema que hace posible el caso Cambridge Analytica, y no tanto en la interferencia concreta del caso en la decisión de voto estadounidense. Para ello, el epígrafe describe el tipo de influencia que ejerce sobre las personas la técnica del *microtargeting*. Seguidamente, cuestiona esta influencia en relación con las limitaciones del modelo utilizado para dibujar el perfil del público objetivo de

dicha campaña, por un lado, y por el otro, de acuerdo con el contexto mediático y sociopolítico actual en el que se inscribe el caso.

Persuasión o manipulación

Según Bennett (2015), la técnica del *microtargeting* incorpora las tendencias que marcan la gestión actual de las campañas electorales en las sociedades occidentales, como el uso de tecnologías *big data* para la recopilación y la integración de los datos de los votantes en plataformas de gestión unificadas, incluyendo sus datos de consumo y los generados en redes sociales, y el paso de los mensajes masivos a los micropúblicos objetivos. Bennett afirma que estas técnicas surgen como resultado de la pérdida de eficacia de las técnicas tradicionales. Son formas más baratas y, a la vez, más intrusivas a la hora de influir en el comportamiento de los votantes. Apunta, también, que estas tendencias están generando una *consumerización* del voto y, por lo tanto, no solo afectan a la privacidad del individuo, sino a dinámicas democráticas más amplias.

Mediante la definición de un perfil individualizado del público, la técnica del *microtargeting* expone al individuo una información determinada de manera selectiva. De este modo, no dice de forma explícita qué consumir o a quién votar, sino que configura algunos de los referentes en relación con los que las personas compran y votan. Por otra parte, que el individuo desconozca qué perfil sobre su persona maneja quien se dirige a él al exponerlo a dicha información coloca a dicho individuo en una situación de vulnerabilidad a la manipulación.

Otra cuestión distinta es que el testimonio de Wiley apunta al uso de técnicas militares de impacto psicológico. Si bien este no es un hecho demostrado, hay dos factores que hacen desconfiar en este sentido: por un lado, la notable similitud entre la oferta de servicios de la empresa Cambridge Analytica (2018) y las características de los ataques informativos perpetrados por las fuerzas de defensa estadounidenses (United States Air Force 1999), y por el otro, la experiencia de SCL Group (2018) en la elaboración de campañas estratégicas de defensa y su vinculación con las élites militares. A esto se le suman los estudios académicos que muestran la potencialidad de los perfiles psicológicos para la elaboración de "operaciones psicológicas".

Un perfil sesgado

El *microtargeting* parte de la definición de un perfil preciso e individualizado del público objetivo. En el caso de la campaña de Trump, este perfil se habría elaborado según el modelo desarrollado por la Universidad de Cambridge (Kosinski, Stillwell y Graepel 2013; Stillwell y Kosinski 2012; Youyou, Kosinski y Stillwell 2015). En este sentido, para hablar de la influencia del caso Cambridge Analytica cabría valorar las posibles limitaciones de dicho modelo.

Las tecnologías *big data* permiten obtener una visión general sobre aquello que se estudia, es decir, una fotografía amplia de la situación. Lo que no está tan claro es que mediante esta fotografía sea posible comprender o explicar fenómenos complejos como la psicología y el comportamiento humanos, que no son matemáticos (boyd y Crawford 2012). Por ello, parece necesario valorar desde un cierto nivel de escepticismo la suposición de que a través del análisis de una determinada representación del comportamiento humano (*likes*) se puede obtener información precisa sobre características complejas de la personalidad (ideología). En este sentido, la aplicación de la analítica *big data* a la conducta humana que se hace en el caso de This is Your Digital Life podría conllevar que los perfiles elaborados sean sesgados. De este modo, la posible influencia ejercida por la campaña de Trump quedaría disminuida.

Contexto mediático

El objetivo aquí es poner en relación la posible influencia de la estrategia de Cambridge Analytica en la decisión de los estadounidenses de votar a Trump o a Clinton con el actual contexto mediático en el que se ha desarrollado la campaña electoral estadounidense.

En un sistema de democracia representativa, la libertad de elección de los representantes políticos es clave. Esto requiere, entre otras cosas, que los ciudadanos tengan acceso a información veraz, diversa y plural. Por ello, los medios tradicionales, pero también los nuevos medios sociales, deben servir como herramientas democratizadoras al servicio del derecho a la libertad de expresión. Sin embargo, la manipulación informativa y la desinformación están en auge y como consecuencia de ello la credibilidad de los medios está en duda (Marwick y Lewis 2017; HLEG 2018).

Marwick y Lewis (2017) argumentan que la desinformación en la red y la radicalización ideológica son consecuencias de la manipulación mediática en la red. Como resultado de un desgaste de la confianza en los medios tradicionales, los principales actores de la manipulación mediática (los *trolls*, los *gamergaters*, los teóricos de la conspiración, los *influencers*, los *haters*, los medios de noticias hiperpartidistas y los políticos) han encontrado su espacio en blogs y webs, foros y tableros de mensajes de internet y en los principales medios sociales (como Facebook, YouTube o Twitter). Según las autoras, estos operan generalmente motivados por razones relacionadas con la ideología, el dinero o la búsqueda de un estatus o de aceptación. Así, la circulación de memes y de bulos, las conspiraciones contra los candidatos, el uso de los *bots* o la distribución de noticias falsas también han jugado un importante papel durante la campaña electoral a las elecciones presidenciales estadounidenses (Marwick y Lewis 2017). Un ejemplo de ello fue la campaña desinformativa promovida en la red acerca de un supuesto pésimo estado de salud de la candidata demócrata, que se hizo viral y saltó a los medios tradicionales.

La evolución de la tecnología *big data* y de la inteligencia artificial ha provocado que la llamada "cultura algorítmica" (Hallinan y Striphas 2016) afecte también a la clasificación y la jerarquización de la información. En los últimos años, el uso de

motores de búsqueda en internet y de los medios sociales para consultar información se ha extendido ampliamente (Nikolov, Oliveira, Flammini y Menczer 2015). En el punto álgido de las elecciones presidenciales en Estados Unidos, un 62% de los ciudadanos se informó a través de las redes sociales (Shearer y Gottfried 2017). Debido a la multiplicación de los dispositivos desde los cuales se accede a la información, los sistemas de recomendación personalizados se han desarrollado como la mejor manera de hacer llegar a los usuarios de internet contenidos informativos acordes a sus intereses (Yingyuan, Pengqiang, Hsu, Hongya y Xu 2015). Numerosos estudios recientes (Borgesius, Trilling, Möller, Bodó, de Vreese y Helberger 2016; Dutton, Reisdorf, Dubois y Blank 2017; Holone 2016; Nikolov, Oliveira, Flammini y Menczer 2015) se han centrado en el impacto de la cultura algorítmica en el auge de la desinformación y la manipulación mediática. La mayoría coinciden en que los ciudadanos se exponen a información sesgada, que confirma y refuerza los pensamientos y actitudes ya adquiridos por uno mismo o por aquellas personas que se consideran "afines" a uno mismo. Este efecto se conoce como "efecto burbuja" (*bubble effect*) o "cámaras de resonancia" (*echo chambers*).

Por otra parte, los medios de comunicación tradicionales siguen desempeñando un importante papel en las campañas electorales. Según Marwick y Lewis (2017), la enmarcación y amplificación estratégica de determinadas ideas o mensajes es una de las técnicas más comunes de manipulación mediática. Patterson (2016) afirma que el tono empleado en la cobertura mediática fue abrumadoramente negativo, mientras que el tratamiento de cuestiones políticas fue extremadamente ligero. No obstante, concluye que la candidata Hillary Clinton fue tratada de una manera más negativa que su contrincante político. Foster Shoaf y Parsons (2016) sostienen que los estereotipos de género siguen perjudicando a las candidatas mujeres en la cobertura mediática de las campañas electorales. Además, la construcción de las marcas políticas (Oates y Moe 2016) o los diferentes usos que ambos candidatos han hecho de las redes sociales (Enli 2017) también tienen un peso importante en la campaña electoral.

Este contexto mediático pone de manifiesto al menos tres cuestiones interesantes para valorar la posible influencia del caso Cambridge Analytica. En primer lugar, que la campaña de *microtargeting* desarrollada por Cambridge Analytica se encuadra en las nuevas formas de manipulación mediática relacionadas con el efecto burbuja. En segundo lugar, que esta no sería la única estrategia de influencia a la que estuvieron expuestos los ciudadanos durante la campaña. Y por último, que los intereses de Trump y Cambridge Analytica no estarían aislados de los intereses del resto de los actores y medios influyentes de la campaña.

Contexto social y político

Entre las explicaciones sugeridas para la victoria de Trump existen muchas otras que no tienen que ver únicamente con la actuación de los medios. Según Gaughan (2016), algunas de ellas estarían relacionadas con las preocupaciones económicas de los votantes blancos de la clase obrera (que la campaña de Trump habría sabido identificar), el auge del racismo y la misoginia, la segregación y la polarización entre el electorado (que, como se ha visto en el epígrafe anterior, podría tener relación con la manipulación informativa), el incremento de la desigualdad en los ingresos, o las polémicas actuaciones del director del FBI. Así, otra cuestión importante a la hora de hablar de la influencia del caso Cambridge Analytica es el contexto político y social en el que se desarrolló la campaña electoral. Fraser (2017) sostiene que la victoria de Trump forma parte de una serie de acontecimientos políticos que se han producido recientemente en el ámbito mundial. Entre ellos señala también el triunfo del *Brexit*, así como la campaña de Bernie Sanders a las primarias del Partido Demócrata estadounidense, el rechazo de las reformas de Matteo Renzi en Italia y el incremento del apoyo al Frente Nacional de Marine Le Pen en Francia. Estos acontecimientos, explica Fraser, representan una oposición ciudadana a los efectos de la globalización, así como a una nueva forma de "neoliberalismo progresista" y a las clases dirigentes que lo han promovido. Trump, señala, captó a una parte del electorado gracias a un "populismo reaccionario" que se oponía a la mezcla de ideales truncados de emancipación y formas letales de *financiarización* que representa el "neoliberalismo progresista".

Conclusiones

La argumentación desarrollada a lo largo de este artículo da lugar, al menos, a las siguientes conclusiones:

1. El caso Cambridge Analytica es la probable consecuencia de una estructura científico-tecnológica, un modelo de negocio y un marco legal determinados que lo hacen posible y necesario.
2. Centrar la atención en el nivel de influencia que haya podido tener la estrategia de Cambridge Analytica en la decisión de voto estadounidense no es útil para comprender la gravedad de la situación por estos cuatro motivos: desvía la atención de las estructuras que lo sustentan y de su impacto social; la influencia de un hecho concreto sobre una decisión compleja es difícil de medir; los sesgos propios del método empleado para elaborar dicha estrategia pueden disminuir dicha influencia, y además, esta sería relativa en relación con su contexto mediático, social y político.
3. La posible influencia ejercida por la campaña de *microtargeting* desarrollada por Cambridge Analytica se inscribe en un fenómeno más amplio de manipulación mediática vinculado a las nuevas tecnologías y al efecto burbuja, y que se ha demostrado como una importante causa del auge de la desinformación en la red y de la radicalización de las ideas y opiniones políticas.

El caso Cambridge Analytica pone de manifiesto que la evolución actual de las tecnologías *big data* genera una situación de desigualdad de poder entre la ciudadanía y un grupo que ejerce un poder despótico sobre la explotación de los datos y la información. Esto afecta a derechos fundamentales como la privacidad, la protección de datos personales o el derecho a la información, y también a la calidad democrática de los estados. Por ello, el presente estudio señala la necesidad de:

1. Reconsiderar el encaje social de las estructuras que catalizan sucesos como el de Cambridge Analytica.
2. No olvidar el impacto social y político de las tecnologías *big data*.
3. Repensar el marco legal de protección de datos personales para corregir sus insuficiencias.
4. Establecer herramientas que permitan al conjunto de la sociedad disponer de información y mecanismos de control sobre las tecnologías *big data*.
5. Imponer barreras, si es necesario, a formas de explotación masiva de datos y/o a los usos que sean perjudiciales para el conjunto de la sociedad.

Referencias

Alkış, N.; Taşkaya Temizel, T. "The impact of individual differences on influence strategies". *Personality and Individual Differences*, 87, 2015, 147-152. doi: 10.1016/j.paid.2015.07.037.

Baruh, L.; Popescu, M. "Big data analytics and the limits of privacy self-management". *New Media & Society*, vol. 19, n.º 4, 2015, 579-596. doi: 10.1177/1461444815614001.

Bennett, C. J. "Trends in voter surveillance in Western societies: privacy intrusions and democratic implications". *Surveillance & Society*, 13 (3/4), 2015, 370-384. <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/voter_surv>.

boyd, d.; Crawford, K. "Critical questions for big data". *Information, Communication & Society*, 15 (5), 2012, 662-679. doi: 10.1080/1369118X.2012.678878.

Borgesius, F. J.; Trilling, D.; Möller, J.; Bodó, B.; de Vreese, C. H.; Helberger, N. "Should we worry about filter bubbles?". *Internet Policy Review*, 5 (1), 2016. doi: 10.14763/2016.1.401.

Briant, E. L. "Pentagon Ju-Jitsu – reshaping the field of propaganda". *Critical Sociology*, 1-18, 5 de marzo de 2018. doi: 10.1177/0896920517750741.

Cadwalladr, C. "'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower". *Observer - The Guardian,* 17 de marzo de 2018. <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump> [Consulta: 23 de abril de 2018].

Cadwalladr, C. "The great British Brexit robbery: how our democracy was hijacked". *Observer - The Guardian*, 7 de mayo de 2017. <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy> [Consulta: 23 de abril de 2018].

Cadwalladr, C.; Graham-Harrison, E. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". *Observer – The Guardian*, 17 de marzo de 2018. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> [Consulta: 23 de abril de 2018].

Cambridge Analytica. *Cambridge Analytica*. 2018. <https://cambridgeanalytica.org/> [Consulta: 23 de abril de 2018].

Dutton, W. H.; Reisdorf, B. C.; Dubois, E.; Blank, G. "Social Shaping of the Politics of Internet Search and Networking: Moving Beyond Filter Bubbles, Echo Chambers, and Fake News". *Quello Center Working Paper*, n.º 2944191, (2017, 1-26. doi: 10.2139/ssrn.2944191.

Enli, G. "Twitter as arena for the authentic outsider: exploring the social media campaigns of Trump and Clinton in the 2016 US presidential election". *European Journal of Communication*, 32 (1), 2017, 50-61. doi: 10.1177/0267323116682802.

Facebook. "¿Cómo puedo averiguar si se ha compartido mi información con Cambridge Analytica?". Servicio de ayuda de Facebook, 2018. <https://www.facebook.com/help/1873665312923476> [Consulta: 18 de abril de 2018].

Foster Shoaf, N.; Parsons, T. N. "18 Million Cracks, but No Cigar: News Media and the Campaigns of Clinton, Palin, and Bachmann". *Social Sciences, MDPI, Open Access Journal*, 5 (3), 2016, 1-15. <https://ideas.repec.org/a/gam/jscscx/v5y2016i3p50-d78592.html>.

Fraser, N. "Progressive Neoliberalism versus Reactionary Populism: A Choice that Feminists Should Refuse". *NORA - Nordic Journal of Feminist and Gender Research*, 24 (4), 2017, 281-284. doi: 10.1080/08038740.2016.1278263.

Gaughan, A. (2016). "Explaining Donald Trump's Shock Election Win". *Scientific American*, 9 de noviembre de 2016. <https://www.scientificamerican.com/article/explaining-donald-trump-s-shock-election-win/>.

Grewal, P. "Suspending Cambridge Analytica and SCL Group from Facebook". *Facebook Newsroom*, 16 de marzo de 2018. <https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/> [Consulta: 18 de abril de 2018].

Hallinan, B.; Striphas, T. "Recommended for you: The Netflix Prize and the production of algorithmic culture". *New Media & Society*, 18 (1), 2016, 117-137. doi: 10.1177/1461444814538646.

Hargittai, E.; Marwick, A. "'What Can I Really Do?' Explaining the Privacy Paradox with Online Apathy". *International Journal of Communication*, 10, 2016, 3737-3757.

High Level Group on Fake News and Online Disinformation. *A multi-dimensional approach to disinformation. Report of the independent High Level Group on fake news and online disinformation*. 2018. <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation> [Consulta: 13 de marzo de 2018].

Holone, H. "The filter bubble and its effect on online personal health information". *Croatian Medical Journal*, 57 (3), 2016, 298-301.

Kosinski, M.; Stillwell, D. J.; Graepel, T. "Private traits and attributes are predictable from digital records of human behavior". *Proceedings of the National Academy of Sciences of the United States of America*, 110 (15), 2013, 5802-5805. doi: 10.1073/pnas.1218772110.

Marwick, A.; Lewis, R. *Media Manipulation and Disinformation Online*. *Data & Society Research Institute*, 2017. <https://datasociety.net/output/media-manipulation-and-disinfo-online/>.

Miralles-Pechuán, L.; Ponce, H.; Martínez-Villaseñor, L. "A novel methodology for optimizing display advertising campaigns using genetic algorithms". *Electronic Commerce Research and Applications*, 27, enero-febrero de 2018, 39-51. Publicado en línea por primera vez en noviembre de 2017. doi: 10.1016/j.elerap.2017.11.004.

Neumann, N. "The power of big data and algorithms for advertising and customer communication". *International Workshop on Big Data and Information Security, IWBIS 2016*, art. n.º 7872882, 2017, 13-14. doi: 10.1109/IWBIS.2016.7872882.

Newman, B. I. *The Marketing Revolution in Politics: What Recent U.S. Presidential Campaigns Can Teach us about Effective Marketing*. Toronto: University of Toronto Press, 2016, 224 páginas.

Nikolov, D.; Oliveira, D. F. M.; Flammini, A.; Menczer, F. "Measuring online social bubbles". *PeerJ Computer Science*, 1 (e38), 2015. doi: 10.7717/peerj-cs.38.

Oates, S.; Moe, W. W. "Donald Trump and the 'Oxygen of Publicity': Branding, Social Media, and Mass Media in the 2016 Presidential Primary Elections". *American Political Science Association Annual Meeting 2016*. doi: 10.2139/ssrn.2830195.

Parlamento Europeo. *Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley* (2016/2225(INI)) ("Implicaciones de los macrodatos en los derechos fundamentales"). <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0076+0+DOC+XML+V0//ES>.

Parlamento Europeo; Consejo de la Unión Europea. *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE ("Reglamento general de protección de datos").* <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES>.

Pasquale, F. *The Black Box Society. The Secret Algorithms that Control Money and Information*. Londres: Harvard University Press, 2015.

Patterson, T. "News Coverage of the 2016 General Election: How the Press Failed the Voters". *Shorenstein Center on Media, Politics and Public Policy at the Harvard Kennedy School*, 7 de diciembre de 2016. <https://shorensteincenter.org/news-coverage-2016-general-election/>.

Rosenberg, M.; Confessore, N.; Cadwalladr, C. "How Trump Consultants Exploited the Facebook Data of Millions". *The New York Times*, 17 de marzo de 2018. <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> [Consulta: 23 de abril de 2018].

Sartonen, M.; Simola, P.; Timonen, J.; Lovén, L. "Ciber personalities as a target audience". *European Conference on Information Warfare and Security, ECCWS,* 2017, 411-418. <https://www.semanticscholar.org/paper/Cyber-Personalities-as-a-Target-Audience-Sartonen-Simola/1cc84c9b9ad74e426aee32828e17c54adad7246a>.

Schroepfer, M. "An Update on Our Plans to Restrict Data Access on Facebook". *Facebook Newsroom*, 4 de abril de 2018. <https://newsroom.fb.com/news/2018/04/restricting-data-access/> [Consulta: 18 de abril de 2018].

SCL Group. *SCL Group*. <https://sclgroup.cc/home> [Consulta: 23 de abril de 2018].

Shearer, E.; Gottfried, J. "News Use Across Social Media Platforms 2017". *Pew Research Centre*, 2017. <http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/> [Consulta: 23 de abril de 2018].

Stillwell, D.J.; Kosinski, M. "myPersonality project: Example of successful utilization of online social networks for large-scale social research". *International Conference on Mobile Systems (MobiSys) 2012.* <www.michalkosinski.com/Stillwell_and_Kosinski_2012.pdf>.

Suárez-Gonzalo, S. "*Big social data*: límites del modelo *notice and choice* para la protección de la privacidad". *El Profesional de la Información*, vol. 26, n.º 2, 2017, 283-292. doi: 10.3145/epi.2017.mar.15.

Tufekci, Z. "Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency". *Colorado Technology Law Journal*, 13, 2015, 203-218.

Turow, J.; Hennessy, M.; Draper, N. *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation".* Annenberg School for Communication University of Pennsylvania, 2015. <https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf>.

United States Air Force. *Psychological Operations. Air Force Doctrine Document 2-5.3*, 27 de agosto de 1999. <http://www.iwar.org.uk/psyops/resources/us/afdd2-5-3.pdf> [Consulta: 19 de abril de 2018].

Yingyuan, X.; Pengqiang, A. I.; Hsu, C.; Hongya, W.; Xu, J. "Time-ordered collaborative filtering for news recommendation". *China Communications*, 12 (12), 2015, 53-62. doi: 10.1109/CC.2015.7385528.

Youyou, W.; Kosinski, M.; Stillwell, D. J. "Computer-based personality judgments are more accurate than those made by humans". *Proceedings of the National Academy of Sciences of the United States of America*, 112 (4), 2015, 1036-1040. doi: 10.1073/pnas.1418680112.

Zuckerberg, M. "I want to share an update on the Cambridge Analytica situation -- including the steps we've already taken and our next steps to address this important issue". Publicación en Facebook, 21 de marzo de 2018. <https://www.facebook.com/zuck/posts/10104712037900071> [Consulta: 18 de abril de 2018].