Revista de Filosofía
Volumen 80 (2023) 215-232

EL BIG DATA EN LOS PROCESOS POLÍTICOS: HACIA UNA DEMOCRACIA DE LA VIGILANCIA[1]

Carlos Saura García
Universitat Jaume I
saurac@uji.es

Resumen / Abstract

Este artículo se centra en el análisis del uso de la industria del *big data* en la política. Se examina de forma pormenorizada el caso de la empresa Cambridge Analytica y se profundiza en los efectos del uso de la tecnología del *big data* en el referéndum de permanencia de Reino Unido en la Unión Europea y en las elecciones presidenciales estadounidenses de 2016. El objetivo es exponer los efectos nocivos que tiene el uso de la tecnología del *big data* en los procesos electorales y los daños que esta tecnología puede producir en los sistemas democráticos.

Palabras clave: *big data*, democracia, vigilancia, Cambridge Analytica, *microtargeting*, psicometría.

Big data in political processes: towards a surveillance democracy

This article will focus on the analysis of the use of the big data industry in the field of politics. This paper will analyze in detail the case of the Cambridge Analytica company and will delve into the effects of the use of big data in the United Kingdom's referendum on permanence in the European Union and in the 2016 US presidential elections. The

[1] Este estudio se enmarca dentro de los objetivos del Proyecto de Investigación Científica y Desarrollo Tecnológico "Bioética cordial y Democracia algorítmica para una sociedad hiperdigitalizada" [PID2022-139000OB-C22], financiado por el Ministerio de Ciencia e Innovación (España). Ha sido posible gracias a la financiación recibida de la Universitat Jaume I a través de un contrato predoctoral (PREDOC/2022/08) y al financiamiento recibidao de la Fundación Balaguer Gonel Hermanos para realizar una estancia de investigación en el CIRSFID-Alma Human AI Centre de la Università di Bologna (Italia).

objective of this article is to show the harmful effects that the use of big data has in electoral contests and the damage that this new technology can cause to democratic systems.

Keywords: big data, democracy, mass surveillance, Cambridge Analytica, microtargeting, psychometry.

1. Introducción

El uso del *big data* en los procesos electorales puede provocar múltiples peligros para el adecuado funcionamiento de la sociedad y de la propia democracia (Mejía 2020). La manipulación de los ciudadanos, la transgresión de la opinión y la vulneración de la libertad de expresión son los principales daños que puede causar el uso inadecuado e invasivo del *big data* en el campo de la política. El *big data* ha hecho que este tipo de manipulación y transgresión ya no se lleve a cabo prohibiendo contenidos o restringiendo libertades, sino por medio de una disposición específica de información, contenidos y noticias adaptadas a las preferencias de los ciudadanos que los consumen (Mejía 2020). El procesamiento de grandes conjuntos de datos ha posibilitado la creación de mensajes y contenidos específicos para cada persona según sus preferencias y sus características (Bennett 2015).

La irrupción del *big data* representó un gran avance en las estrategias y acciones de persuasión política, pero el avance de mayor importancia se produjo en el momento que las nuevas posibilidades de los datos masivos permitieron realizar una segmentación psicográfica de la ciudadanía (Stillwell y Kosinski 2012; Kosinski *et al*. 2013; Youyou *et al*. 2015). La combinación de los beneficios de la segmentación psicográfica y del análisis de grandes conjuntos de datos ha permitido utilizar las limitaciones cognitivas de las personas y la personalización de contenidos para tergiversar y manipular la libertad de expresión de la población (Suárez Gonzalo 2018). Los denominados sesgos cognitivos son usados para influenciar el pensamiento de los ciudadanos de una forma disimulada, pues afectan a la totalidad de la ciudadanía y están vinculados con los errores comunes de la mente que conducen a la generación de interpretaciones subjetivas e imperfectas de la información (Kahneman 2011). Estos sesgos son inofensivos en el día a día de los ciudadanos, pero de forma inconsciente dan lugar a formas de actuar irracionales. En el campo de la psicología se han observado una gran variedad de sesgos cognitivos, algunos de ellos son tan sutiles que a los ciudadanos les resulta difícil darse cuenta de que están obrando de forma irracional (Lakoff 2004; Kahneman 2011).

El uso de estos sesgos cognitivos en el ámbito de la política afecta de una manera prácticamente imperceptible a los votantes y consigue influenciarlos de manera decisiva en sus opiniones (Arceneaux 2012). La personalización de la información da lugar a una versión sesgada de la realidad adecuada a la forma de ser de cada individuo, este fenómeno genera contextos en los que se potencian determinadas ideologías y puntos de vista que acaban provocando consecuencias nocivas para los sistemas democráticos (González 2017). La continua exposición de determinados puntos de vista y opiniones provoca que solo se tenga en cuenta una perspectiva de la realidad, lo que causa una limitación premeditada de la información y de los hechos que restringe la capacidad de razonar de los ciudadanos (Sunstein 2001).

El objetivo de este artículo es mostrar los efectos nocivos que tiene el uso del *big data* en las contiendas electorales y el daño que esta tecnología causa a los sistemas democráticos. Para lograr este propósito, se examina el uso del *big data* en las acciones y estrategias de persuasión política, se estudian las nuevas técnicas de manipulación e intoxicación social y se profundiza en el caso de la empresa Cambridge Analytica y el uso del *big data* en la campaña electoral a favor del *brexit* en el referéndum de permanencia del Reino Unido en la Unión Europea y en la campaña electoral de Donald Trump en las elecciones presidenciales de Estados Unidos de 2016.

2. Manipulación política y big data

La combinación del fenómeno del *big data*, de las limitaciones cognitivas de las personas y de la personalización de contenidos en los procesos democráticos permite influir de forma decisiva sobre los votantes indecisos y consigue que estas personas se identifiquen con una determinada ideología. Las tecnologías vinculadas al fenómeno del *big data* han superado las regulaciones y los marcos legales y han originado un nuevo modelo de comunicación política basado en el pensamiento irracional y en la evasión de la cognición, esta nueva política amenaza seriamente los fundamentos de los sistemas democráticos (Mejía 2020).

Las investigaciones psicométricas realizadas por científicos de la Universidad de Cambridge basadas en el análisis de datos masivos fueron uno de las innovaciones más destacadas en el uso del *big data* en el ámbito de la política (Stillwell y Kosinski 2012; Kosinski *et al*. 2013; Youyou *et al*. 2015). Estos estudios permitieron realizar una predicción del comportamiento y de las características de las personas a partir de las actividades y las reacciones de los usuarios de la plataforma social Facebook.

Inicialmente, Kosinski *et al*. (2013) mostraron que con un promedio de 68 *likes* (“me gusta” en castellano) de un usuario de la red social Facebook se

podía predecir su ideología (85% de precisión), su orientación sexual (88% de precisión), su color de piel (95% de precisión), y también su consumo de alcohol, su religión, su inteligencia, etc. Posteriormente, Youyou *et al*. (2015) llevaron a cabo un estudio en el que se evidenció que un algoritmo era capaz de realizar una predicción de la conducta humana con una fiabilidad muy elevada a partir de los *likes* de Facebook. Con diez *likes* este algoritmo podía predecir el comportamiento de una persona con mayor precisión que un compañero de trabajo, con cincuenta *likes* mejor que un miembro de su familia y con trescientos *likes* mejor que su propia pareja. Estas investigaciones se basan en el procesamiento de grandes cantidades de *likes* de multitud de usuarios de Facebook. Es importante destacar que los *likes* no desprenden mucha información, sino que solo muestran que algún contenido le llama la atención, le gusta o le disgusta a un usuario, hay que subrayar también que los *likes* son reacciones públicas: hasta hace poco tiempo para poder verlos no era necesario estar en contacto con el usuario que los había emitido ni tampoco tener una cuenta en la red social Facebook.

El desarrollo de la tecnología del *big data* se ha acelerado en los últimos años, actualmente ya no hay necesidad de analizar la actividad de los usuarios en las redes sociales para predecir su personalidad, solo se necesita analizar los gustos musicales (Nave *et al*. 2018) o las particularidades del rostro de una persona (Wang y Kosinski, 2018) para descubrir las singularidades y predecir la personalidad de las personas. Los denominados GAMAM (Google, Amazon, Meta, Apple y Microsoft) dominan el espacio de internet y recolectan una gran cantidad de datos que les permite predecir la personalidad de los ciudadanos y manipularlos en función de sus propios intereses, el enorme poder de estas compañías pone en serio riesgo el buen funcionamiento de la opinión pública (González de la Garza 2018). La facilidad con la que las grandes compañías tecnológicas pueden predecir las conductas y las características de los ciudadanos a partir de pequeños detalles de la vida digital de estos muestran la sencillez con la que se puede controlar a la sociedad (Suárez Gonzalo 2019).

Los instrumentos creados por los científicos de la Universidad de Cambridge permiten la creación de perfiles psicológicos con los datos de la ciudadanía y también la búsqueda de perfiles específicos (Mejía, 2020). Este hecho supone el nacimiento de un mecanismo de búsqueda de personas que puede ser de gran utilidad en los procesos electorales para localizar a los ciudadanos con ciertas características emocionales o ideológicas, como, por ejemplo, aquellos que no tienen claro por quién votar o las personas con características emocionales específicas. El fenómeno del *big data* se ha convertido en un elemento esencial de la nueva política, el procesamiento de grandes cantidades de datos personales procedentes de internet hace posible conocer de forma detallada las características de los ciudadanos (Suárez Gonzalo 2019). Si se combina la capacidad predictiva de la industria del *big data* con el análisis de grandes bases de datos recopiladas por el sector comercial, la policía, los gobiernos o los poderes fácticos es posible conocer

el nombre, la localización, la edad, la personalidad y los intereses de millones de ciudadanos del mundo (Mejía 2020).

Las innovaciones desarrolladas por la industria del *big data* han originado el denominado *microtargeting* y la propaganda electoral cognitiva. La propaganda computacional ha supuesto una gran evolución respecto de la propaganda tradicional y se ha convertido en una parte fundamental del actual contexto digital (Woolley y Howard 2017). Esta nueva propaganda se denomina también propaganda activa o inteligente debido a que se centra en los sesgos cognitivos, las características y las emociones de la ciudadanía para crear campañas propagandísticas especialmente diseñadas para las preferencias de cada uno de los votantes.

El *microtargeting* es el nuevo modelo de publicidad automatizada centrada en buscar personas específicas para ofrecerles determinada propaganda adaptada a sus características. Este nuevo formato publicitario tiene la capacidad de aprender de las reacciones de las personas y perfeccionar la propaganda basándose en la situación emocional de los ciudadanos y en la interacción entre los contenidos de la propaganda automatizada y los propios ciudadanos en un diálogo virtual (González de la Garza 2018). El objetivo del *microtargeting* es agrupar a los electores en pequeños segmentos sincronizados con los distintos perfiles psicométricos para así dirigir los contenidos de la propaganda electoral y conseguir que la publicidad personalizada alcance su objetivo e influya sobre la opinión de los votantes. Actualmente es habitual observar que en cualquier búsqueda en internet posterior a visitar un comercio virtual nos aparezcan ofertas o anuncios de los productos que hemos visitado con anterioridad, este tipo de publicidad se realiza a partir de las denominadas *cookies* (López Jiménez, 2011). Las *cookies* son la forma de publicidad automatizada equivalente al *microtargeting* electoral pero en la dimensión comercial. La gran diferencia entre estos *microtargeting* es que el electoral aprende de la interacción de la persona a la que tratará de influir por medio de argumentos emocionales que imitan sus intereses personales y sociales y con variantes de una campaña publicitaria amoldada a su perfil psicológico (González de la Garza 2018).

La técnica del *microtargeting* expone unos contenidos especialmente seleccionados para cada uno de los ciudadanos, pero esta información en ningún momento muestra de forma explícita qué producto comprar o a qué candidato votar, sino que crea un contexto informativo favorable a estos objetivos adaptado al perfil de cada uno (Suárez Gonzalo 2018). La propaganda computacional ha creado un nuevo modelo de ingeniería social destinado a manipular la opinión pública de la ciudadanía y se ha convertido en uno de las herramientas más poderosas en contra del correcto funcionamiento de la democracia (Bond *et al*. 2012; Woolley y Howard 2017). El *microtargeting* y la propaganda electoral cognitiva no son los únicos fenómenos que ponen en riesgo la democracia: las redes de distorsión de la opinión pública basadas en la introducción de tendencias en la redes sociales y la macrodifusión de contenidos falsos para moldear la opinión pública son otras prácticas nocivas para los procesos democráticos (D'Ancona, 2019).

Las redes de distorsión de la opinión pública están creadas e impulsadas por personas, empresas o conglomerados influyentes a nivel nacional e internacional capaces de alterar el flujo informativo de los principales temas de interés político por medio de la manipulación de tendencias (González de la Garza 2018). Esta manipulación es posible gracias a la creación de *hashtags* en Twitter, Facebook o Instagram para sobredimensionar informaciones y opiniones por medio de los llamados *trending topics*. Esta estructura de tergiversación de la opinión pública se basa en el procesamiento de grandes cantidades de datos de las redes sociales y en la distribución estratégica de contenidos en determinados sectores de la ciudadanía. Estas tendencias distorsionadoras son creadas de una manera completamente artificial y deliberada por granjas de ordenadores o *bots* automatizados al servicio de los grupos de interés y son consentidas por las condiciones de uso de las propias redes sociales (Howard *et al*. 2018). Además de las redes de distorsión de la opinión pública, observamos también otro fenómeno relacionado con la propaganda cognitiva y el uso del *big data*, esta es la industria de las noticias falsas (*fake news* en inglés).

Las *fake news* tienen la misma manera de funcionar que las redes de distorsión y los mecanismos de procesamiento de datos masivos de la propaganda cognitiva, pero en este caso las informaciones que se propagan no intentan convencer a la ciudadanía, sino confundirla. Pauner Chulvi (2018) afirma que las noticias falsas son contenidos e informaciones publicados en las plataformas digitales de comunicación que carecen de fuentes reconocidas, que no han sido comprobadas ni verificadas y que su principal objetivo es la manipulación de la sociedad a partir de la creación de inseguridades, la desestabilización de apoyos o la desacreditación. Las *fake news* se basan en mensajes cortos con provocativos titulares basados en imágenes y videos destinados a introducir informaciones relacionadas con la posverdad en el contexto informativo, estos contenidos tienen un impacto directo en la opinión pública (Zafra 2017). La estructura de las noticias falsas y la rápida y exponencial expansión dificultan –incluso podríamos decir imposibilitan– refutarlas y desmentir las falsedades de dicha información. Un ejemplo del uso de *fake news* en contiendas democráticas es la campaña sobre inmigración que hicieron algunos promotores del *leave* en el referéndum del *brexit*. Algunas candidaturas favorables a la salida de la Unión Europea realizaron una difusión de imágenes y videos en las redes sociales en las que se podía observar una gran cola de refugiados intentando entrar en Europa. Esta campaña tuvo un gran impacto sobre la ciudadanía británica, pues sus contenidos se vinculaban de forma directa con una crisis migratoria en la Unión Europea. A pesar de que las imágenes y los videos difundían una información totalmente falsa, tuvieron un gran impacto en la opinión pública y fueron determinantes en la victoria de la opción favorable a la salida de la Unión Europea (D'Ancona 2019).

El uso de estas nuevas técnicas relacionadas con el fenómeno del *big data* amenazan de forma clara la libertad de la población debido a que limitan el derecho fundamental a la información, promueven contenidos dedicados a manipular a la ciudadanía e introduce informaciones para tergiversar la opinión pública (Dutton

et al. 2017). En esta línea, Nix (2016) afirma que la industria de los datos masivos ha dado lugar a una comunicación política centrada en la personalización de los contenidos y en la distorsión de la esfera pública para conseguir decantar a los ciudadanos hacia una determinada opinión. Las nuevas posibilidades del *big data* en el ámbito social y político entraña grandes peligros relacionados con la libertad de expresión, la manipulación de la sociedad y la privacidad de la población.

La debilidad de las norma de protección de datos y la violación de la privacidad de los ciudadanos por medio de la extracción de datos mediante los objetos con Internet de las cosas (IoT) incorporado, el gran poder conseguido por las grandes empresas tecnológicas gracias al procesamiento de datos de millones de ciudadanos y la capacidad de descubrir las peculiaridades de cada individuo de la sociedad gracias a la extracción y procesamiento de sus datos han creado un contexto en el cual la ciudadanía está constantemente vigilada. Las consecuencias de este contexto están creando una red de vigilancia social similar a la descrita por George Orwell en su libro *1984* (2013) en el que los pensamientos, las conductas y las actividades de las personas eran totalmente predecibles y controlables (González 2017; Lyon 2018). El actual clima de vigilancia y control total sobre la población pone en riesgo los pilares del sistema democrático e invierte los valores principales de la democracia (Keane 2013). La capacidad de vigilar a la población que tienen las grandes compañías y los centros de poder está originando una inversión de las reglas democráticas, en vez de ser las personas quienes monitoreen a las grandes compañías y los centros de poder, son estos los que controlan los pensamientos y las actividades de la ciudadanía. La gran irrupción de las innovaciones tecnológicas y de la industria del *big data* en los procesos democráticos está dando lugar a un nuevo modelo democrático: la llamada democracia de la vigilancia.

En el siguiente apartado se dará cuenta del uso de la industria del *big data* para interferir en contiendas electorales en un caso práctico: las actividades y las estrategias ocupadas por el conglomerado de empresas denominado SCL Group y, en especial, por la empresa Cambridge Analítica en la victoria del *leave* en el referéndum de permanencia de Reino Unido en la Unión Europea de 2016 y en la victoria de Donald Trump en las elecciones presidenciales estadounidenses de 2016. En estos casos, se observan los grandes riesgos que comporta el uso de las nuevas posibilidades de los datos masivos para la sociedad y para la democracia, entre los que destacan el excesivo poder de las grandes empresas tecnológicas en la nueva economía global dominada por los datos, la extracción de información privada de los ciudadanos y el uso de las tecnologías de los datos masivos para manipular los procesos electorales.

3. El uso del big data en los procesos democráticos: el caso de Cambridge Analytica

Cambridge Analytica fue una sociedad filial de SCL Group con sede en Nueva York, Washington y Londres fundada en 2013. La actividad principal de Cambridge Analytica se centraba en elaborar operaciones de comunicación estratégica con la finalidad de alterar la opinión de grupos concretos de la población en favor de determinados objetivos. Para ello, esta empresa investigaba a cierto grupo de ciudadanos para descubrir sus características principales; extraía datos de este público y los introducía en bases, analizaba segmentos sociales propensos a responder favorablemente a contenidos y llevaba a cabo campañas específicas para afectar estos segmentos clave de la ciudadanía (Berghel 2018). A continuación, nos centraremos en las estrategias y procedimientos usados por Cambridge Analytica y las otras empresas filiales de SCL Group en los procesos democráticos del Reino Unido y los Estados Unidos en el año 2016.

El factor clave de las acciones tomadas por este grupo de empresas en estos procesos electorales fue la filtración de datos privados de 87 millones de usuarios de la red social Facebook en el año 2014, de estos 87 millones alrededor de 70 millones eran perfiles de ciudadanos de los Estados Unidos y un millón eran de ciudadanos británicos (Schroepfer 2018). El testimonio de Christopher Wylie, exempleado y *whistleblower* de Cambridge Analytica, publicado en *The Guardian* (Cadwaladr 2018a; Cadwaladr y Graham-Harrison, 2018) y en *The New York Times* (Rosenberg *et al*. 2018), destapó que la sustracción de esta gran cantidad de datos se realizó gracias al trabajo del profesor del Departamento de Psicología de la Universidad de Cambridge, Aleksandr Kogan. El trabajo de Kogan se centró en emular la aplicación de Facebook de análisis psicométrico *myPersonality,* desarrollada con finalidades académicas y cuyas conclusiones fueron publicadas en el año 2012 (Stillwell y Kosinski 2012).

La aplicación creada por Kogan fue bautizada como *This is Your Digital Life*, la nueva plataforma basada en la realización de test de personalidad a los usuarios de Facebook empezó a funcionar en el 2014. Los usuarios aceptaban compartir los datos de sus perfiles para fines académicos a cambio de dos o tres dólares de recompensa económica, pero en realidad esta información fue usada con el objetivo de analizar las características de la ciudadanía para manipularla políticamente. Alrededor de trescientas mil personas hicieron la prueba de personalidad y permitieron que esta aplicación recopilara una gran cantidad de datos vinculados a sus actividades y a su perfil en Facebook (cantidad de *likes*, cumpleaños, género, ubicación y preferencias, entre otros). Pero el aspecto más importante de esta aplicación tenía que ver con que las prácticamente inexistentes leyes de privacidad de la red social Facebook también permitían acceder y extraer estos conjuntos de datos de los amigos de los

usuarios que realizaron el test de personalidad, aumentando la sustracción de datos hasta 87 millones de perfiles en todo el mundo (Vercelli 2018).

La empresa Cambridge Analytica y las otras filiales del SCL Group usaron los métodos desarrollados por Stillwell y Kosinski (2012), Kosinski *et al*. (2013) y Youyou *et al*. (2015) para realizar análisis psicométricos con los datos recogidos por la aplicación *This is Your Digital Life*, creada por Kogan. Tal y como se ha explicado anteriormente, el análisis de los registros digitales de los usuarios de Facebook, como, por ejemplo, la información del perfil o los *likes,* permitieron descubrir características ocultas de las personas. En Rosenberg *et al*. (2018), el *whistleblower* Christopher Wylie explicó que gracias a estos nuevos procedimientos Cambridge Analytica consiguió una descripción detallada de afinidades políticas y perfiles psicológicos de millones de usuarios de Facebook. Wylie (2019) expone que para completar el trabajo de procesamiento de datos Cambridge Analytica utilizó información de bases de datos internas de diversas empresas para combinar la ya recopilada información psicológica y política de las personas con correos electrónicos, teléfonos y direcciones postales, obteniendo de esta forma una detallada base de datos sobre millones de ciudadanos del mundo. Estos bancos de datos contenían una amplia amalgama de información: desde el perfil psicológico del ciudadano, el estado de salud o la cantidad de dinero que tenía en el banco, hasta el trabajo que realizaba, la fotografía de su rostro, la localización de su casa o la música que le gustaba. Esta información hizo posible recrear las vidas de las personas y actualizarlas instantáneamente gracias a un programa digital cuyo objetivo era persuadir y manipular a la población.

Antes de usar los procedimientos de *big data* manipulativo en el referéndum del *brexit* y en las elecciones presidenciales estadounidenses del 2016, Cambridge Analytica ejecutó campañas de manipulación política en procesos electorales de países subdesarrollados como Nigeria, Trinidad y Tobago, Moldavia y Ucrania para comprobar el funcionamiento adecuado de las técnicas de procesamiento de grandes conjuntos de datos y de los métodos de manipulación política (Wylie 2019). Una vez confirmada la efectividad de estos procedimientos, Cambridge Analytica y las diversas filiales del SCL Group comenzaron a llevar a cabo campañas de persuasión y manipulación en importantes contiendas electorales alrededor del mundo: cooperaron con el candidato republicano Ted Cruz en las elecciones primarias de su partido, participaron en la campaña a favor de la salida en el referéndum de permanencia del Reino Unido en la Unión Europea y fueron fundamentales en la victoria de Donald Trump en las elecciones presidenciales estadounidenses. A continuación, se profundiza en la participación de Cambridge Analytica y del SCL Group en la victoria del *leave* en el referéndum del *brexit* y en la victoria de Donald Trump en las elecciones presidenciales estadounidenses: se analizan las operaciones de manipulación social, las técnicas empleadas y cómo estos procedimientos afectaron al resultado de estas contiendas electorales.

3.1. Referéndum de permanencia de Reino Unido en la Unión Europea

En este referéndum, el SCL Group colaboró con las campañas políticas *Leave.eu* (relacionada con el partido de extrema derecha UKIP) y *Vote Leave* (relacionada con el partido conservador) para que el Reino Unido abandonara la Unión Europea, por medio de sus empresas subsidiarias Cambridge Analytica y AggregatedIQ (Cadwaladr 2017b). El multimillonario empresario británico a favor del *brexit*, Arron Banks, fue el principal financiador de las operaciones realizadas por el SCL Group durante esta contienda electoral. Las leyes del Reino Unido prohibían la cooperación en más de una campaña de apoyo al *brexit*, en un principio el SCL Group solo participaba en la campaña vinculada al UKIP, pero gracias a un entramado de sociedades a nivel mundial consiguió sortear la legislación y también participó en *Vote Leave* (Cadwaladr 2017b).

Los principales impulsores del *brexit* sabían que era necesario expandir la base social de este movimiento para ganar el referéndum, por este motivo era de suma importancia captar la mayor cantidad de votos posibles de personas de una ideología política diferente a la conservadora. Cambridge Analytica se dedicó a identificar a los potenciales votantes del partido laborista, a las personas simpatizantes de otros partidos y a los ciudadanos que no tenían intención de votar con la finalidad de persuadirlos para que votaran a favor del *brexit* o para que no fueran a votar (Wylie 2019). El principal objetivo del trabajo de Cambridge Analytica era manipular a la mayor cantidad de votantes no conservadores que fuera posible. Kaiser (2019) expone que Cambridge Analytica usó y combinó múltiples bases de datos con el propósito de descubrir los conjuntos de votantes más vulnerables y realizar operaciones de *microtargeting* y distorsión informativa enfocadas hacia esos grupos.

Por una parte, ejecutó una campaña de *microtargeting* dirigida hacia un grupo específico de votantes indecisos con posibilidades de votar a favor de la salida del Reino Unido (Wylie 2019). El análisis de las particularidades de este grupo de votantes por medio del *big data* reveló dos grandes preocupaciones: las cuestiones vinculadas con la justicia social y el trato de los extranjeros procedentes de países de la Commonwealth. La campaña *Vote Leave* desarrolló una rama de propaganda progresista llamada *BeLeave* que se centró en la introducción de contenidos y noticias relacionados con temas como la igualdad de trato de los inmigrantes, la discriminación de los ciudadanos procedentes de fuera de la Unión Europea y la protección del medioambiente (Cadwaladr 2018b). Wylie (2019) expone que en las semanas previas a la celebración del referéndum esta campaña emitió más de cien anuncios *online* diferentes con miles de mensajes distintos dependiendo de las emociones y de las características de cada votante. Esta campaña se centró en un segmento vulnerable de votantes progresistas y durante los días previos al referéndum sus contenidos fueron vistos más de ciento setenta millones de veces en la red.

Por otra parte, se realizó una gran inversión para hacer una campaña de distorsión informativa por medio de la introducción en las redes sociales de *fake news* e informaciones de dudosa veracidad. Estos contenidos se centraban en cuestiones relacionadas con la inmigración y con la economía (D'Ancona 2019). En cuanto a la inmigración, el contenido de estas campañas exponía que la permanencia en la Unión Europea potenciaba una emigración de trabajadores poco cualificados hacia el Reino Unido que mermaba la calidad de vida de los ciudadanos británicos y que la posible incorporación de Turquía a la Unión Europea provocaría una avalancha de refugiados. Respecto de la economía, se difundieron noticias en las que se informaba que el coste semanal de pertenecer a la Unión Europea era de 350 millones de libras, que la mayor parte del presupuesto de la Unión Europea se destinaba a pagar los salarios de los funcionarios de las instituciones europeas y que la inversión procedente de la Unión Europea en el Reino Unido era mucho menor que la inversión de otras naciones. Una encuesta llevada a cabo por la empresa Ipsos en junio de 2016 refleja el impacto de este tipo de afirmaciones sobre la opinión pública: los británicos creían que el porcentaje de presupuesto de la Unión Europea destinado a pagar a los sueldos de los funcionarios era un 27% cuando en realidad era solo un 6%, que las inversiones europeas en el Reino Unido representaba el 30% del total cuando en realidad era el 48% y que la inversión procedente de China representaba el 19% del total cuando en realidad solo representaba el 1% (Ipsos 2016). La repetición de forma masiva de afirmaciones de este tipo centrada en un sector específico de la ciudadanía con características psicográficas agresivas produjo un clima de rabia e indignación que disminuyó la necesidad de obtener explicaciones racionales (Craker y March 2016) y dio lugar a un ambiente distorsionado favorable para el avance de las candidaturas del *leave*.

El trabajo de manipulación social realizado por Cambridge Analytica y AggregatedIQ gracias a la filtración de información privada de los usuarios de Facebook, al procesamiento de grandes cantidades de datos de diversas bases de datos y a las campañas de contaminación y distorsión informativa personalizadas consiguió influenciar a la opinión pública británica. El movimiento a favor del *brexit*, por medio de las campañas manipulativas dirigidas hacia determinados segmentos vulnerables de votantes progresistas y la introducción de *fake news* en las redes sociales, logró crear una contradictoria alianza entre votantes progresistas, inmigrantes y votantes conservadores antiinmigración (Wylie 2019). Los resultados del referéndum arrojaron una ajustada victoria de la opción de abandonar la Unión Europea con el 51,89% de los votos. Esta victoria subrayó la importancia de las redes sociales en los procesos electorales y el enorme poder de manipulación de la industria del *big data*. Esta fue la primera gran victoria electoral en la que participó Cambridge Analytica y el preludio de su participación en la campaña de Donald Trump en las elecciones presidenciales de los Estados Unidos.

3.2. Elecciones presidenciales estadounidenses de 2016

Cambridge Analytica comenzó sus operaciones de manipulación política en los Estados Unidos participando en la campaña de Ted Cruz en las elecciones primarias del partido republicano, la compañía usó estas primarias para testear el correcto funcionamiento de sus técnicas y mejorar su funcionamiento. Ted Cruz fue derrotado y Donald Trump logró la nominación como candidato del partido republicano. Luego, el equipo de Donald Trump decidió contratar los servicios de Cambridge Analytica. En las elecciones presidenciales de 2016, Donald Trump se enfrentó a la candidata del partido demócrata, Hillary Clinton. El trabajo de Cambridge Analytica en esta elecciones se basó en tres grandes estrategias: *microtargeting* enfocado hacia los potenciales votantes del partido republicano, una campaña de inflamación social de los simpatizantes de Donald Trump a nivel nacional y una operación de supresión de voto centrada en los votantes demócratas (Wylie 2019).

La capacidad de conocer las características emocionales y personales de los votantes estadounidenses gracias a los análisis psicográficos y al procesamiento de grandes conjuntos de datos revolucionó la campaña de Donald Trump (Rodríguez-Andrés, 2018). Esta información permitió llevar a cabo operaciones de *microtargeting* enfocadas hacia los votantes indecisos y los simpatizantes del partido republicano. El nuevo *microtargeting* dejó obsoleta la tradicional diferenciación de los grupos de votantes (hombres, mujeres, blancos, afroamericanos, ricos, pobres, etc.) y permitió una segmentación individualizada basada en las peculiaridades de cada ciudadano (Bennett 2015). Junto al *microtargeting*, se ejecutaron estrategias de inflamación social y de supresión de voto.

Cambridge Analytica creó una campaña de inflamación política por medio de Facebook y de su algoritmo que desencadenó un aumento de la ira de la ciudadanía (Rodríguez-Andrés 2018). Para esta campaña, la empresa generó páginas con nombres relacionados con la ideología del partido republicano y gracias al funcionamiento del algoritmo interno de Facebook estas páginas aparecieron en las recomendaciones de otros usuarios que habían dado *like* a contenidos parecidos. A medida que los usuarios se introducían en estas páginas, se difundían contenidos seleccionados sobre la base de las características de los miembros del grupo y de esta forma aumentar la irritación y conseguir un mayor compromiso con la candidatura de Donald Trump. Inicialmente, se crearon grupos a nivel local, después a nivel estatal y finalmente a nivel nacional. Estas páginas fueron el motor de una gran plataforma de radicalización ideológica, propagación de noticias falsas y distorsión informativa en las redes sociales a favor del candidato republicano (Wylie 2019). Paralelamente a las campañas de atracción de votantes, también se dirigieron operaciones hacia los simpatizantes del partido demócrata.

Estas acciones sobre los potenciales votantes demócratas fueron las denominadas operaciones de supresión de votos (*voter supresion* en inglés). El objetivo era poner

en duda las capacidades y aptitudes de Hillary Clinton para ser presidenta de los Estados Unidos e influir sobre los ciudadanos para que votaran por el candidato de un tercer partido o para que no fueran a votar (Ravel 2018). Estas acciones se dirigieron a votantes blancos liberales, mujeres jóvenes y afroamericanos. Para desarrollar esta campaña, Cambridge Analytica difundió una gran cantidad de anuncios negativos en las redes sociales, adaptados al perfil psicográfico de las personas de cada uno de estos grupos, en los que se exponían noticias de dudosa veracidad sobre la campaña del partido demócrata, aspectos discutidos de la vida de Hillary Clinton o directamente *fake news* (Guess *et al*. 2018). Allcott y Gentzkow (2017) estudiaron el uso de las *fake news* en este proceso electoral y constataron el excelente trabajo de distorsión informativa: a lo largo de los últimos tres meses de campaña electoral las noticias falsas que circulaban en Facebook y beneficiaban a Donald Trump se compartieron treinta millones de veces, mientras que las *fake news* favorables a Hillary Clinton solo se difundieron ocho millones de veces. Las operaciones de *microtargeting* y las acciones de inflamación política en las redes sociales se incrementaron durante las semanas previas a las elecciones y fueron decisivas para la victoria de Donald Trump (Kaiser 2019). Los resultados de las elecciones presidenciales le otorgaron 304 congresistas a Donald Trump y 227 a Hillary Clinton, con estos resultados el candidato republicano logró la presidencia de los Estados Unidos.

La extracción de grandes conjuntos de datos de Facebook, el desarrollo de las técnicas de procesamiento de datos masivos y las estrategias de publicidad personalizada y la distorsión informativa permitieron a la empresa Cambridge Analytica crear una maquinaria de manipulación democrática sin precedentes en la historia (Wylie 2019). Las inversiones multimillonarias del empresario Robert Mercer fueron fundamentales para conseguir este propósito (Cadwaladr 2017a). Mercer es un científico informático estadounidense que ganó grandes cantidades de dinero a través de programas y tecnologías vinculadas con la inteligencia artificial y fue director ejecutivo del famoso fondo de inversión Renaissance Technologies. Es mundialmente conocido por ser simpatizante de la ideología política ultraconservadora, pues financió múltiples campañas del partido republicano e invirtió grandes cantidades de dinero en el portal de noticias ultraconservador *Breitbart*. Vistas las grandes posibilidades comerciales y políticas que tenían las nuevas técnicas de análisis y manipulación social mediante el *big data*, Robert Mercer decidió financiar al SCL Group, conglomerado de empresas al que pertenecía Cambridge Analytica (Wylie 2019). La implicación de Robert Mercer en las campañas electorales de Ted Cruz y de Donald Trump hicieron que Cambridge Analytica colaborara con estos candidatos y sus amistades entre los partidos conservadores británicos en la campaña del *brexit* (Cadwaladr 2017a). Las grandes campañas propagandísticas en las redes sociales financiadas por Robert Mercer en la candidatura de Donald Trump y por Arron Banks en la campaña del brexit fueron esenciales para la manipulación de los votantes y la consecución de sus objetivos a nivel político (Cadwaladr 2017b).

El clima de constante vigilancia en el que vive actualmente la sociedad está afectando negativamente a la democracia (Zuboff 2015; Lyon 2018). La industria del big data está amenazando la privacidad de los ciudadanos, todas sus acciones, emociones y pensamientos son constantemente analizados y procesados con finalidades comerciales o políticas (Gil 2016; Polo Roca 2020). Los denominados GAMAM han conseguido un enorme poder económico y manipulativo gracias a la gran cantidad de datos personales que los usuarios introducen en sus plataformas (Miguel de Bustos y Izquierdo-Castillo 2019). Los poderes fácticos utilizan el actual contexto digital para introducir de forma interesada determinadas ideologías en la opinión pública y de esta forma manipular los procesos democráticos (Cadwaladr 2017a). El denominado capitalismo de la vigilancia (Zuboff 2015) ha transformado la democracia y ha creado un nuevo formato democrático: la llamada democracia de la vigilancia.

4. Conclusiones

El desarrollo de las herramientas de vigilancia de la población y de los instrumentos de manipulación social permite a los poderes fácticos y a las grandes empresas tecnológicas modelar la opinión de los ciudadanos y la ideología de la sociedad (Marwick y Lewis 2017; Miguel de Bustos y Izquierdo-Castillo 2019). Las grandes corporaciones tecnológicas, los poderes fácticos y los multimillonarios realizan operaciones de manipulación ideológica de la sociedad para conseguir sus objetivos como se ha visto claramente en la victoria del *leave* en el referéndum de permanencia del Reino Unido en la Unión Europea y en la victoria de Donald Trump en las elecciones presidenciales estadounidenses del 2016 (Cadwaladr 2017a y 2017b).

Las características de la democracia de la vigilancia suponen un gran riesgo para el adecuado funcionamiento del actual sistema democrático. La estructura de vigilancia social basada en la extracción y análisis de grandes conjuntos de datos de millones de personas procedentes de internet, de las redes sociales y de aparatos con Internet de las cosas (IoT), ha permitido conocer de forma detallada las características, las emociones y las opiniones de los ciudadanos en cada instante de su vida. El uso de esta información por parte de los poderes fácticos y de las grandes empresas tecnológicas para la realización de operaciones de manipulación política diseñadas específicamente para cada persona representa una gran amenaza para el correcto funcionamiento de la democracia. La manipulación social ha sido utilizada repetidas veces a lo largo del tiempo, pero el potencial manipulativo de la tecnología del *big data* supera con creces cualquier mecanismo utilizado anteriormente. El uso de las innovaciones tecnológicas y comunicativas de la sociedad de la información con finalidades nocivas para la ciudadanía ha permitido crear una maquinaria de manipulación a nivel mundial que ha convertido a la ciudadanía en una mera transmisora de los intereses y de las ideologías de los personajes multimillonarios,

las grandes empresas y las oligarquías. Este hecho ha disminuido la importancia de la ciudadanía y ha colocado a estos colectivos en una posición central dentro del sistema democrático.

El mantenimiento del poder de la ciudadanía en los procesos electorales y la defensa de los beneficios de los sistemas democráticos son aspectos trascendentales en la sociedad actual. El actual contexto de vigilancia social y el uso de innovadoras tecnologías de manipulación política ha instaurado una plutocracia encubierta en la que las decisiones políticas son tomadas por los poderes fácticos, pero siempre legitimadas en procesos electorales por una ciudadanía manipulada para conseguir estos propósitos. La reversión del clima de control y vigilancia social que existe en la actualidad y la prohibición de las técnicas de manipulación política basadas en la tecnología del *big data* es esencial para la recuperación del poder de la ciudadanía y el buen funcionamiento del sistema democrático.

Referencias bibliográficas

Allcott, Hunt y Gentzkow, Matthew (2017), "Social media and fake news in the 2016 election", en *Journal of Economic Perspectives*. 31.2: 211-236. https://doi.org/10.1257/jep.31.2.211.

Arceneaux, Kevin (2012), "Cognitive Biases and the Strength of Political Arguments". *American Journal of Political Science*. 56.2: 271-285. https://doi.org/10.1111/j.1540-5907.2011.00573.x.

Bennett, Colin J. (2015), "Trends in voter surveillance in western societies: Privacy intrusions and democratic implications". *Surveillance and Society*. 13.3-4: 370-384. https://doi.org/10.24908/ss.v13i3/4.5373.

Berghel, Hal. (2018), "Malice Domestic: The Cambridge Analytica Dystopia". *Computer*. 51.5: 84-89, https://doi.org/10.1109/MC.2018.2381135.

Bond, Robert M.; Fariss, Cristopher J.; Jones, Jason J.; Kramer, Adam D. I.; Marlow, Cameron; Settle, Jaime E. y Fowler, James H. (2012), "A 61-million-person experiment in social influence and political mobilization". *Nature*. 489: 295-298, https://doi.org/10.1038/nature11421.

Cadwaladr, Carole (2017a), "Robert Mercer: the big data billionaire waging war on mainstream media". *The Guardian*, Londres, 26 de febrero. https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage.

____ (2017b), "The great British Brexit robbery: how our democracy was hijacked", en *The Guardian*, 17 de marzo. https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

____ (2018a), "I made Steve Bannon's psychological warfare tool': meet the data war whistleblower" *The Guardian*, 17 de marzo. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

____ (2018b), "The Brexit whistleblower: 'Did Vote Leave use me? Was I naive?'", en *The Guardian*, 28 de marzo. https://www.theguardian.com/uk-news/2018/mar/24/brexit-whistleblower-shahmir-sanni-interview-vote-leave-cambridge-analytica.

Cadwaladr, Carole y Graham-Harrison, Ema (2018), "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". *The Guardian*, 17 de marzo, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Craker, Naomi y March, Evita (2016), "The dark side of Facebook®: The Dark Tetrad, negative social potency, and trolling behaviours". *Personality and Individual Differences*. 102: 79-84, https://doi.org/10.1016/j.paid.2016.06.043.

D'Ancona, Matthew (2019), *Posverdad: La nueva guerra en torno a la verdad y cómo combatirla*. Madrid: Alianza.

Dutton, William H.; Reisdorf, Bianca C.; Dubois, Elizabeth y Blank, Grant (2017), "Search and Politics: The Uses and Impacts of Search in Britain, France, Germany, Italy, Poland, Spain, and the United States", *Quello Center Working Paper*. https://dx.doi.org/10.2139/ssrn.2960697

Gil, Elena (2016), *Big data, privacidad y protección de datos*. Madrid: Agencia Estatal Boletín Oficial del Estado.

González de la Garza, Luis M. (2018), "La crisis de la democracia representativa. Nuevas relaciones políticas entre democracia, populismo virtual, poderes privados y tecnocracia en la era de la propaganda electoral cognitiva virtual, el microtargeting y el Big Data". *Revista de Derecho Político*. 103: 257-302. https://doi.org/10.5944/rdp.103.2018.23203.

González, Roberto J. (2017), "Hacking the citizenry?: Personality profiling, 'big data' and the election of Donald Trump". *Anthropology Today*. 33.3: 9-12. https://doi.org/10.1111/1467-8322.12348.

Guess, Andrew; Nyhan, Brendan y Reifler, Jason (2018), "Selective exposure to misinformation: Evidence from the consumption of fake news during the 2016 US presidential campaign". *Exeter*, 9 de enero.

Howard, Philip N.; Woolley, Samuel y Calo, Ryan (2018), "Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration". *Journal of Information Technology and Politics*. 15.2: 81-93. https://doi.org/10.1080/19331681.2018.1448735.

Ipsos (2016), "*The Perils of Perception and the EU*", *Ipsos Mori*, 9 de junio. https://www.ipsos.com/ipsos-mori/en-uk/perils-perception-and-eu.

Kahneman, Daniel (2011), *Thinking, fast and slow*. Nueva York: Farrar, Straus & Giroux Inc.

Kaiser, Brittany (2019), *Targeted: My Inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy*. Londres: HarperCollins.

Keane, John (2013), *Democracy and media decadence*. Cambridge: Cambridge UP.

Kosinski, Michal; Stillwell, David y Graepel, Thore (2013), "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: 5802-5805. https://doi.org/10.1073/pnas.1218772110.

Lakoff, George (2004), *Don't think of an Elephant*. Vermont: Chelsea Green Publishing.

López Jiménez, David (2011), "Las cookies como instrumento para la monitorización del usuario en la Red: la publicidad personalizada". *Revista de Ciencias Económicas*. 29.2: 175-190.

Lyon, David (2018), *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press.

Marwick, Alice y Lewis, Rebecca (2017), *Media Manipulation and Disinformation Online*. New York: Data & Society Research Institute.

Mejía, Andrés Fernando (2020), "La libertad de expresión en jaque, el panóptico del Siglo XXI. Big Data como amenaza para la democracia: a propósito del caso Cambridge Analytica". *Revista de Filosofía, Derecho y Política*. 32: 79-105. https://doi.org/10.20318/universitas.2020.5512.

Miguel de Bustos, Juan C. e Izquierdo-Castillo, Jessica. (2019). "¿Quién controlará la Comunicación? El impacto de los GAFAM sobre las industrias mediáticas en el entorno de la economía digital". *Revista Latina de Comunicación Social*. 74: 803-821. https://doi.org/10.4185/RLCS-2019-1358.

Nave, Gedeón; Greenberg, David M.; Kosinski, Michal; Stillwell, David y Rentfrow, Jason (2018), "Musical Preferences Predict Personality: Evidence from Active Listening and Facebook Likes". *Pyschological Science*. 29.7: 1145-1158. https://doi.org/10.1177/0956797618761659.

Nix, Alexander (2016), *Cambridge Analytica - The Power of Big Data and Psychographics*, Concordia Annual Summit, 19 y 20 de septiembre. https://www.youtube.com/watch?v=n8Dd5aVXLCc.

Orwell, George (2013). *1984*. Madrid: Penguin Random House.

Pauner Chulvi, Cristina. (2018). "Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la red". *Teoría y Realidad Constitucional*. 41: 297-318.

Polo Roca, Andoni (2020), "Sociedad de la información, sociedad digital, sociedad de control". *Inguruak*. 68: 50-77.

Ravel, Ann (2018), "A New Kind of Voter Suppression in Modern Elections". *University of Memphis Law Review*, 49.4: 1019-1064.

Rodríguez-Andrés, Roberto (2018), "Trump 2016: ¿presidente gracias a las redes sociales?". *Palabra Clave*. 21.3: 831-859. https://doi.org/10.5294/pacla.2018.21.3.8.

Rosenberg, Matthew; Confessore, Nicholas y Cadwaladr, Carole (2018), "How Trump Consultants Exploited the Facebook Data of Millions". *The New York Times*, 17 de marzo. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

Schroepfer, Mike (2018), "An Update on Our Plans to Restrict Data Access on Facebook". *Facebook Newsroom*, 4 de abril. https://newsroom.fb.com/news/2018/04/restricting-data-access/.

Stillwell, David y Kosinski, Michal (2012), "myPersonality project: Example of successful utilization of online social networks for large-scale social research". *International Conference on Mobile Systems (MobiSys)*, 25 de junio.

Suárez-Gonzalo, Sara (2018), "Tus likes ¿tu voto? Explotación masiva de datos personales y manipulación informativa en la campaña electoral de Donald Trump a la presidencia de EE.UU. 2016". *Quaderns del CAC*. 21.44: 27-36.

____ (2019), "Big data, poder y libertad sobre el impacto social y político de la vigilancia masiva". Tesis doctoral, Universitat Pompeu Fabra, http://www.tdx.cat/handle/10803/668235.

Sunstein, Cass R. (2001), *Republic.com 2.0*. Princeton: Princeton UP.

Vercelli, Ariel (2018), "La (des)protección de los datos personales: análisis del caso Facebook Inc.-Cambridge Analytica". *Simposio Argentino de Informática y Derecho (SID)*: 1-12.

Wang, Yilun y Kosinski, Michal (2018), "Deep neural networks are more accurate than humans at detecting sexual orientation from facial images". *Journal of Personality and Social Psychology*. 114.2: 246-257, https://doi.org/10.1037/pspa0000098.

Woolley, Samuel C., y Howard, Philip N. (2017), "Computational Propaganda Worldwide: Executive Summary". *Computational Propaganda Research Project*. Oxford: Oxford UP; pp. 1-15.

Wylie, Christopher (2019), *Mindf*ck. Inside Cambridge Analytica's Plot to Break the World.* Londres: Profile Books.

Youyou, Wu; Kosinski, Michal y Stillwell, David (2015), "Computer-based personality judgments are more accurate than those made by humans". *Proceedings of the National Academy of Sciences*. 112.4: 1036-1040. https://doi.org/10.1073/PNAS.1418680112.

Zafra, Remedios (2017), "Redes y posverdad", en *En la era de la posverdad*. Barcelona: Calambur; pp. 181-192.

Zuboff, Shoshana (2015), "Big other: Surveillance capitalism and the prospects of an information civilization", en *Journal of Information Technology*. 30.1: 75-89. https://doi.org/10.1057/jit.2015.5.