Daimon. Revista Internacional de Filosofía, nº 93 (2024), pp. 73-89
ISSN: 1130-0507 (papel) y 1989-4651 (electrónico) http://dx.doi.org/10.6018/daimon.609851

Microtargeting político y vigilancia social masiva: impactos negativos en las democracias occidentales*

Political microtargeting and mass social surveillance: negative impacts on western democracies

*CARLOS SAURA GARCÍA***

Resumen: Este artículo se centra en los peligros para los procesos democráticos de uno de los principales instrumentos de propaganda política, el llamado *microtargeting* político. Este tipo de *microtargeting* permite dirigir contenidos específicos, hacia votantes específicos, en momentos específicos y vincularlos directamente con sus características, sesgos y vulnerabilidades individuales. El objetivo de este artículo es exponer el funcionamiento y los diversos tipos de *microtargeting* político y mostrar las posibles consecuencias nocivas de esta técnica en los procesos democráticos. Para lograr este objetivo, por una parte, se detallará la extracción, explotación y utilización de grandes conjuntos de datos para la creación de diversos tipos de propaganda política personalizada y, por otra parte, se analizarán las diversas propuestas existentes para limitar los

Abstract: This article focuses on the dangers to democratic processes of one of the main instruments of political propaganda, the so-called political microtargeting. This type of microtargeting allows you to direct specific content, towards specific people, at specific times and link them directly to their individual characteristics, biases, and vulnerabilities. The objective of this article is to expose the operation and the various types of political microtargeting, show the harmful consequences of this technique on democratic processes and propose solutions to address these negative consequences. To achieve this objective, on the one hand, the extraction, exploitation, and use of large data sets for the creation of various types of personalized political propaganda will be detailed and, on the other hand, the various existing proposals will be analyzed to limit the

Recibido: 26/03/2024. Aceptado: 18/06/2024.

* Esta publicación es parte del proyecto PID2022-139000OB-C22, financiado por MCIU/AEI/10.13039/501100011033/FEDER, UE y ha sido posible gracias a la financiación recibida de la Universitat Jaume I a través de un contrato predoctoral (PREDOC/2022/08).

** Investigador predoctoral en el departamento de Filosofía y Sociología de la Universitat Jaume I (UJI) de Castellón. Mis líneas de investigación se centran en el estudio de los efectos de las nuevas tecnologías del *big data* sobre la sociedad, profundizando especialmente en tres campos: retos éticos de la *datificación* y la hiperconectividad, implicaciones de los GAMAM (Google, Amazon, Meta, Apple y Microsoft) en el tratamiento y utilización de los datos masivos e implicaciones éticas de la utilización de los datos masivos en las contiendas democráticas y en los sistemas democráticos (*mass democracy*). Publicaciones recientes: Saura García, C. (2023). El big data en los procesos políticos: hacia una democracia de la vigilancia. *Revista de filosofía*, *80*, 215-232. https://doi.org/10.4067/S0718-43602023000100215 y Saura García, C. (2024). Digital expansionism and big tech companies: consequences in democracies of the European Union. *Humanities and Social Sciences Communications*, *11*(448), 1-8. https://doi.org/10.1057/s41599-024-02924-7

efectos negativos que puede causar el *microtargeting* político y para mejorar el funcionamiento de las democráticas occidentales.
Palabras clave: microtargeting, ecosistemas ciberfísicos, dataficación, capitalismo de la vigilancia, vigilancia social masiva

negative effects that can cause political microtargeting and to enhance the functioning of Western democracies.
Keywords: microtargeting, cyberphysical ecosystems, datafication, surveillance capitalism, mass social surveillance

Introducción

Los llamados ecosistemas *ciberfísicos* se han convertido en los elementos clave de la infraestructura digital de las sociedades modernas. Estos hacen posible la hibridación de los fenómenos de la digitalización, la *hiperconectividad*, la *dataficación* y la *algoritmización* y permiten la obtención de valor a partir de grandes conjuntos de datos (Calvo, 2021). Estos ecosistemas se podrían definir como la recreación de espacios artificiales solapados a aplicaciones, programas, dispositivos e instrumentos informáticos, biométricos o sensoriales interconectados y controlados por algoritmos que hacen posible la *hiperconectividad* y la *dataficación* de la totalidad de la realidad física y digital del comportamiento, las actividades, y las preferencias de personas, animales, objetos o procesos (Armenteras et al., 2016; Calvo, 2020). Los procesos de estos ecosistemas *ciberfísicos* permiten generar de forma continua grandes cantidades de datos; almacenar y procesar los conjuntos de datos para convertirlos en información, conocimiento y valor; y finalmente por medio de algoritmos aplicar esta información, conocimiento y valor para afectar e incidir en la realidad (Calvo, 2021).

Las grandes corporaciones tecnológicas del planeta (Google, Amazon, Meta, Apple, Microsoft, Alibaba, Baidu, Tencent, Huawei, etc.) obtienen grandes cantidades de beneficios económicos, vinculados en la mayoría de casos a la publicidad, gracias a la implementación del modelo de negocio del capitalismo de la vigilancia y a la explotación comercial y publicitaria de los ecosistemas *ciberfísicos* (Zuboff, 2020). Se estima que el valor del mercado de la publicidad global durante el año 2019 fue de 319 billones de dólares y se espera que este valor alcance los 1089 billones de dólares en 2027 (Galli et al., 2022). Pero esta explotación no está exenta de aspectos dañinos para la sociedad y especialmente para la democracia. Deibert (2019) subraya que este modelo de negocio esconde "tres dolorosas verdades". La primera es que este mercado está construido en base a la invasión de la privacidad de los ciudadanos y a su monetización. La segunda es que los propios ciudadanos son cómplices y conscientes de este nivel de vigilancia social masiva realizada por estas corporaciones y de la explotación de sus datos. Y la tercera y última, es que el modelo de negocio publicitario no es ni mucho menos incompatible con la manipulación y el autoritarismo. En relación a los efectos dañinos para la democracia, Calvo (2019) expone que:

> El neuromarketing político y económico, por ejemplo, puede utilizar los ecosistemas *ciberfísicos* para diseñar e implementar campañas altamente adictivas, capaces de modular y/o manipular la voluntad libre de los sujetos del sistema, así como de menguar o inhibir la capacidad crítica de votantes, gobernantes y clientes con el objetivo de maximizar el beneficio particular de unos pocos. (p.12)

Este fragmento pone en evidencia el enorme potencial manipulativo que pueden atesorar los ecosistemas *ciberfísicos*. Los diferentes actores interesados en influir en los procesos electorales y en el sistema democrático en general se han dado cuenta del enorme potencial de los grandes conjuntos de datos y han desarrollado innovadoras tecnologías para adaptar sus mensajes propagandísticos (Hersh, 2015; Wylie, 2019; Da Empoli, 2020; Schick, 2020; Woolley, 2023). Esta situación ha provocado la creación de una infraestructura de propaganda computacional capaz de crear contenidos altamente personalizados para influir específicamente en determinados segmentos de la sociedad basándose en los patrones extraídos de los grandes conjuntos de datos de los ecosistemas *ciberfísicos* (Howard, 2020; Dawson, 2021; Woolley, 2023).

La rápida evolución de los ecosistemas *ciberfísicos* ha hecho posible la aparición del denominado *microtargeting* político en estos entornos (Woolley y Howard, 2018). El *microtargeting* político es un tipo de propaganda computacional automatizada y *algoritmizada* que tiene el objetivo de seleccionar a ciudadanos específicos y ofrecerles una propaganda política activa que pueda influir y manipular su comportamiento, sus opiniones y su ideología. La principal característica de esta propaganda es su capacidad de aprender a partir de las interacciones con los ciudadanos y afinarse a través del dialogo virtual entre los propios ciudadanos y los contenidos de la propaganda computacional (Bashyakaria et al., 2019)[1].

El objetivo de este artículo será exponer los efectos negativos que el *microtargeting* político puede tener sobre los procesos democráticos de las sociedades modernas. En un primero momento, se analizará los procesos de extracción y explotación de datos que alimentan la tecnología del *microtargeting*. A continuación, se expondrán los diversos tipos de *microtargeting* y las peculiaridades de cada uno de ellos. Finalmente se profundizará en la situación existente en las democracias de las sociedades occidentales y se analizaran las diversas propuestas existentes para limitar los efectos negativos causados por el *microtargeting* político y mejorar el funcionamiento de los sistemas democráticos.

1. Vigilancia social masiva: extracción y explotación de grandes conjuntos de datos

Actualmente el *microtargeting* está estrechamente vinculado con los fenómenos de la vigilancia social masiva y la recolección indiscriminada de datos (Dawson, 2021, 2023). El modelo de negocio del capitalismo de la vigilancia ha desarrollado un tejido de vigilancia social masiva centrado en la *datificación* de la totalidad de los aspectos de la ciudadanía y de las sociedades con el objetivo de capturar la mayor cantidad de datos posibles de todas las acciones que se realizan en el mundo para posteriormente extraer valor de estos y obtener beneficios económicos (Ebeling, 2022).

La aplicación práctica de este tejido de vigilancia social masiva supone la extracción de datos de una vasta cantidad de aspectos, actividades, comportamientos y procesos del día a día de la ciudadanía, como por ejemplo la *datificación* de la información relativa a navega-

1 Es importante destacar que el embrión del *microtargeting* político se encuentra en la disciplina de la psicotecnia. Schumpeter (1958) fue uno de los primeros pensadores en exponer que la psicotecnia electoral —basada en técnicas y métodos psicológicos y sociológicos— podía ser utilizada para influir y moldear el comportamiento electoral en procesos democráticos.

ción en la red (Bashyakaria et al., 2019), las compras online y en la vida real (Llaneza, 2019) o las operaciones realizadas con tarjetas de crédito (Mayer-Schönberger y Cukier, 2013). Pero también otros procesos extractivos más dañinos para la privacidad y la intimidad de la ciudadanía como son la *datificación* de la intimidad corporal (Farahany, 2023), la voz (Turow, 2021), los rostros (De Miguel, 2024), la ubicación de los smartphones (Thompson y Warzel, 2019) y la extracción de datos y metadatos privados a través de aplicaciones destinadas al entretenimiento de niños (Fowler, 2022a) o a través de diversos dispositivos digitales como son el asistente virtual, la Smart TV, la nevera, el microondas, la aspiradora, las luces inteligentes e incluso el inodoro (Fowler, 2022b).

La gran cantidad de datos y metadatos extraídos de forma continua por parte de la maquinaria del capitalismo de la vigilancia ha otorgado la posibilidad a cualquier persona con unos conocimientos mínimos de navegación en la red y de análisis de datos de tener "direct access to the minds and lives of guards, clerks, girlfriends… a detailed trail of personal information that would perviously have taken months of careful oberservation to gather" (Wylie, 2019: 49). Un claro ejemplo de la facilidad de explotar, segmentar y extraer valor de grandes conjuntos de datos es el trabajo final de grado que realizaron dos estudiantes de la Escuela de Ingeniería y Ciencias Aplicadas John A. Paulson de Harvard (Zewe, 2020). Estos estudiantes fueron capaces a través de un conjunto de datos robados a la compañía de informes de crédito Experian con información privada de 6 millones de personas en relación con 69 variables diferentes (dirección, número de teléfono, donaciones a partidos políticos, correo electrónico, contraseñas, hijos, etc.) que encontraron en la *dark* web de descubrir y recrear perfiles característicos de tres senadores, tres diputados de la Cámara de Representantes y el alcalde de Washington DC y sus miembros de gabinete, en los cuales se incluyan informaciones como las calificaciones crediticias, los números de teléfono y las direcciones. La facilidad con la que estos estudiantes totalmente amateurs fueron capaces de identificar características de individuos específicos pone en evidencia el potencial que pueden tener la realización de este tipo de técnicas por profesionales y corporaciones con una tecnología mucho más potente y con unos conjuntos de datos mucho más grandes y actualizados.

En el campo de la política este tipo de técnicas permite atomizar e *hipersegmentar* grandes bases de datos e identificar a personas específicas en contextos específicos para aplicarles propaganda política personalizada, es decir, *microtargeting* político, con el objetivo de persuadirlas y manipularlas políticamente de la forma más precisa y eficaz posible (Matz et al., 2017; Nave et al., 2018; Kosinski, 2021).

Las primeras referencias de utilización de *microtargeting* político en entornos *ciberfísicos* datan de las campañas electorales presidenciales de Barack Obama en 2008 y 2012[2]. En estas dos contiendas se construyó y se desarrolló una infraestructura de creación de perfiles en base a las características de las personas y de búsqueda de perfiles específicos a partir

2 Cabe señalar que el *microtargeting* político ya existía previamente a la utilización masiva de las plataformas digitales por medio de técnicas de marketing directo. Las primeras referencias de utilización de marketing directo datan de las décadas de 1960 y 1970 en los EEUU. Estas técnicas fueron introducidas por el publicista Richard Viguiere en el Partido Republicano y se enfocaron a la creación de bases de datos de direcciones de los ciudadanos, la segmentación de votantes y la personalización de mensajes (Moriyama, 2022). Sus efectos fueron determinantes para la victoria del candidato republicano Ronald Reagan en las elecciones presidenciales de 1980.

de la adquisición de conjuntos de datos a las grandes corporaciones tecnológicas y a *data brokers* (Issenberg, 2012; Bimber, 2014; Gerodimos y Justinussen, 2015). Esta infraestructura era aún embrionaria y bastante básica, pero fue ampliamente desarrollada y utilizada por el equipo de campaña de Donald Trump en las elecciones presidenciales de 2016 y por el equipo del Brexit en el referéndum de permanencia de Reino Unido en la Unión Europea (UE) en 2016 (Kaiser, 2019; Wylie, 2019).

En estas dos contiendas la empresa especializada en operaciones de comunicación estratégica Cambridge Analytica fue capaz de recrear los perfiles psicológicos y las afinidades políticas de millones de personas actualizadas al instante gracias a sus perfiles de Facebook (Kaiser, 2019; Wylie, 2019)[3]. El *whistleblower* de la empresa Cambridge Analytica, Christopher Wylie, reveló que estos perfiles psicológicos y afinidades políticas fueron utilizados para realizar multitud de campañas de *microtargeting* político para persuadir y manipular a la población por medio de las denominadas operaciones psicológicas (Wylie, 2019)[4]. El estrecho margen de la victoria de Donald Trump en algunos importantes estados (diferencias menores al 1% de los votos en los estados de Michigan, Wisconsin y Pensilvania), y de la victoria del Brexit (diferencia de un 3,78% entre los votos a favor y en contra), ponen de manifiesto lo decisivas que pudieron ser estas campañas de *microtargeting* para el resultado final de estas contiendas (Jamieson, 2018; Wylie, 2019).

Durante los últimos 5 años algunas grandes corporaciones digitales y algunos estados han empezado a desarrollar las reglamentaciones en relación a privacidad y protección de los datos de sus usuarios y sus ciudadanos (Galli, 2021; Fässler, 2023), especialmente después del descubrimiento por parte de la opinión pública en 2018 de las prácticas de extracción de datos realizada de forma ilícita por Cambridge Analytica a través de Facebook y la puesta en marcha de propaganda computacional basada en psicometría (Cadwalladr, 2017; Cadwaladr y Graham-Harrison, 2018; Rosenberg et al., 2018). Como consecuencia de la actualización y desarrollo de las reglamentaciones puestas en marcha por las grandes corporaciones digitales y los gobiernos, se han buscado nuevas formas de extraer datos y metadatos de la ciudadanía para posteriormente poner en marcha campañas de persuasión y manipulación política a través de *microtargeting*.

En el caso de las elecciones presidenciales de los Estados Unidos (EEUU) de 2020, tanto Joe Biden como Donald Trump utilizaron *apps* oficiales de campaña con la finalidad de extraer datos de los ciudadanos (Woolley y Gursky, 2020). En el ciclo político americano iniciado en 2016 los candidatos utilizaron las grandes plataformas digitales para extraer datos y manipular a los votantes (Kaiser, 2019; Wylie, 2019). En el ciclo político que empezó en 2020 esta función se ha trasladado a las aplicaciones oficiales de campaña. Woolley y Gursky (2020) subrayan que estas *apps*:

3 Esto fue posible gracias a una filtración de datos privados de 87 millones de usuarios de Facebook en 2014 y a la combinación de estos datos con bases de datos de consumidores adquiridas a compañías especializadas en la compra-venta de datos (Kaiser, 2019; Wylie, 2019).

4 Durante este tiempo la empresa Cambridge Analytica también realizó campañas de manipulación electoral en otros países como Nigeria, Trinidad y Tobago, Moldavia o Ucrania (Wylie, 2019).

> […] allow the Trump and Biden teams to speak directly to likely voters. They also allow them to collect massive amounts of user data without needing to rely on major social-media platforms or expose themselves to fact-checker oversight of particularly divisive or deceptive messaging.

Este fragmento pone en evidencia que el principal objetivo de estas aplicaciones es la extracción indiscriminada de datos y metadatos de sus usuarios, y de los contactos de estos usuarios, sin depender de terceras partes. Los permisos de extracción de datos solicitados por estas plataformas para poder ser utilizadas, en el caso de la *app* de Joe Biden, incluían obligatoriamente el número de teléfono, el código postal, el correo electrónico, los contactos, la información de las búsquedas en internet o las redes Wifi; mientras que en el caso de la *app* de Donald Trump a esta lista se le sumaban multitud de permisos de extracción de datos como son la ubicación, la obtención de información privada del propio *smartphone* y de la tarjeta SD o la información relativa al Bluetooth (Woolley y Gursky, 2020).

Las aplicaciones de campaña se han convertido en un elemento más de la infraestructura del capitalismo de la vigilancia dedicada a afectar a los procesos democráticos. Estas aplicaciones permiten obtener a los candidatos flujos de datos actualizados directamente de sus simpatizantes más afines y de todos sus contactos, y posteriormente combinarlos con multitud de conjuntos de datos comprados a las grandes corporaciones digitales o a empresas dedicadas al negocio de compra-venta de datos como Acxiom, Resonate, i360 o Targetsmart para de esta forma crear microsegmentos de ciudadanos con características similares e identificar a personas específicas en contextos específicos para intentar persuadirlas y manipularlas con *microtargeting* político (Bartlett et al., 2018; Bashyakaria et al., 2019; Woolley y Gursky, 2020).

2. La sala de máquinas del *microtargeting* político

A partir del proceso continuo de extracción y explotación de grandes conjuntos de datos de la ciudadanía y de la sociedad en general, los algoritmos proceden a crear, seleccionar y enviar las informaciones más adecuados para persuadir y manipular a cada persona. En este punto es fundamental enviar de la forma más sutil, eficiente y eficaz posible argumentos, contenidos y propaganda política que se adapten al máximo posible a los intereses personales, sociales, psicológicos o emocionales de cada persona, a los diversos contextos y circunstancias de la vida diaria de la ciudadanía y a las variaciones de estos. El objetivo del *microtargeting* político es persuadir y manipular la opinión, la ideología y la intención de voto de determinados ciudadanos en favor de los intereses de quien lo ejecuta (Bashyakaria et al., 2019). Este tipo de *microtargeting* abarca diversos métodos para lograr, por una parte, unos niveles de adaptación y personalización máximos y, por otra parte, unos niveles de persuasión y manipulación máximos para cada persona (Matz et al., 2017; Bashyakaria et al., 2019; Bakir, 2020; Iyer et al., 2021). Entre estos métodos destacan:

— El *A/B testing*
— El *geotargeting*
— El *psicotargeting*
— El targeting cognitivo
— El *neurotargeting*

El *A/B testing* hace referencia a un tipo de *microtargeting* en el cual se comparan dos o más variables de un mismo argumento, contenido o propaganda para, de esta forma, maximizar el impacto que tiene sobre cada ciudadano (Bashyakaria et al., 2019)[5]. El *A/B testing* utiliza los datos y metadatos extraídos de la ciudadanía y la sociedad para, en un primer momento, seleccionar a determinados segmentos de la ciudadanía a los cuales va a afectar y, posteriormente, optimizar los contenidos para incrementar su poder de persuasión y manipulación (Bashyakaria et al., 2019). El objetivo de este método es interactuar con los votantes y adaptarse a sus características a través de contenidos automatizados únicos, personalizados y actualizados constantemente gestionados por algoritmos, los cuales crean, combinan y modifican una amplia variedad de botones, textos, imágenes y videos para aumentar la eficacia y la eficiencia de los contenidos enviados.

El *geotargeting* está vinculado con la utilización de datos y metadatos acerca de la ubicación para enviar argumentos y contenidos determinados y propaganda personalizada (Iyer et al., 2021). La combinación de los datos de la ubicación de las personas con otros conjuntos de datos, como pueden ser datos en relación con actividades físicas, compras, características sociales, contactos o actividad en las redes sociales, permite conocer los intereses, opiniones, costumbres y deseos de cada persona en cada momento e incrementar la precisión de los argumentos, contenidos y propaganda enviados. Las dos principales variantes de aplicación del *geotargeting* son el *geofencing* y el *IP targeting*.

El *geofencing* fija un perímetro virtual alrededor de un determinado punto y promociona un determinado mensaje con unas características específicas a las personas que se encuentran en el interior o que se acercan hacia él gracias a sus datos en relación a ubicación, Bluetooth, etc. (Bashyakaria et al., 2019; Woolley y Gursky, 2020; Iyer et al., 2021). El *IP targeting* se basa en el envío de mensajes con argumentos y contenidos personalizados a direcciones IP de determinados dispositivos conectados a la red especialmente seleccionadas para lograr unos niveles de persuasión y manipulación máximos en las personas que los usan (Bashyakaria et al., 2019; Iyer et al., 2021; Singer, 2022).

El *psicotargeting* es el tipo de *microtargeting* que utiliza la información psicológica de la ciudadanía para crear perfiles psicológicos de cada persona, buscar perfiles específicos entre la población y personalizar, optimizar y mejorar las campañas de persuasión y manipulación política basándose en las peculiaridades psicológicas de cada ciudadano (Matz et al., 2017; Bashyakaria et al., 2019; Bakir, 2020). La posibilidad de analizar grandes conjuntos de datos heterogéneos de cada ciudadano gracias a innovadoras herramientas psicométricas ha permitido predecir de forma detallada y actualizada la personalidad, los estados de ánimo o las emociones de cada persona en cada momento[6]. Entre estas herramientas destacan la predicción de la personalidad a través de *likes* de Facebook (Kosinski et al., 2013; Youyou et al., 2015), las preferencias musicales (Nave et al., 2018) o una imagen del rostro de las

5 Un ejemplo de utilización de *A/B testing* es la utilización por parte de la candidatura de Donald Trump a las elecciones presidencial de EEUU de 2016 de entre 50.000 y 60.000 variaciones diarias de la mismo anuncio político en Facebook (Bartlett et al., 2018; Da Empoli, 2020).

6 Estas herramientas psicométricas en la mayoría de los casos toman como referencia el modelo OCEAN, también llamado modelo de los cinco grandes rasgos de personalidad, en el cual se valora la personalidad de cada persona teniendo en cuenta la apertura, responsabilidad, extroversión, amabilidad e inestabilidad emocional (Gerber et al., 2011).

personas (Kosinski, 2021; De Miguel, 2024). En muchos casos el *psicotargeting* político se lleva a la práctica por medio de las llamadas operaciones psicológicas (*psychological operations* o PSYOPS en inglés). Las PSYOPS son un tipo de propaganda, normalmente utilizada por ejércitos en conflictos bélicos, de tipo manipulativo que incide en las vulnerabilidades emocionales y en los estados de ánimo (Haig y Hajdu, 2017).

El targeting cognitivo utiliza los datos vinculados con los sesgos cognitivos, es decir, los errores imperceptibles del cerebro a la hora de generar interpretaciones informativas incompletas, imperfectas y defectuosas que dan lugar a formas de actuar y opinar irracionales, para enviar argumentos, contenidos y propagandas determinadas con el objetivo de afectar de forma disimulada a la ciudadanía e influir y manipular de forma decisiva su ideología y sus opiniones (Kahneman, 2011; Mercier y Sperber, 2017; Sanborn y Harris, 2018). Entre los sesgos cognitivos más comunes destacan el sesgo de punto ciego, el sesgo de apoyo a la elección, el sesgo de anclaje, el sesgo de confirmación, la ilusión de agrupamiento, el efecto *Bandwagon*, el sesgo innovativo o el sesgo de actualidad (Kahneman, 2011; Juárez Ramos, 2019).

El *neurotargeting* está basado en la extracción y explotación de los datos de la intimidad corporal de las personas, es decir, datos vinculados a la información biométrica e íntima como son las ondas cerebrales, la presión sanguínea, la actividad electrodérmica o la electromiografía facial[7]. En el ámbito de la política esta técnica busca crear marcos, contenidos, estímulos o impulsos con el objetivo de persuadir y manipular a las personas e influir en la autonomía, la cognición y la libertad de los ciudadanos de forma prácticamente imperceptible.

La puesta en marcha de un *microtargeting* político capaz de crear multitud de variables de un mismo contenido, de actualizar y optimizar estas variables dependiendo de la ubicación de las personas, de las peculiaridades psicológicas, de beneficiarse de las limitaciones cognitivos y de utilizar información biométrica e íntima ha permitido crear una propaganda computacional automatizada y *algoritmizada* basada en la personalización, la imperceptibilidad, la evasión de la cognición y la potenciación del pensamiento irracional capaz de manipular a la ciudadanía y poner en serio riesgo los principios básicos de la democracia (Han, 2021). La utilización del *microtargeting* político puede manipular la voluntad política de la ciudadanía, afectar directamente a la soberanía de la ciudadanía y adulterar los procesos democráticos (Da Empoli, 2020; Zuboff, 2020; Han, 2021). Ante esta amenaza para la democracia, algunos estados han empezado a fortalecer y desarrollar la reglamentación en relación con la extracción y análisis de grandes conjuntos de datos y con el envío de propaganda computacional personalizada (Galli et al., 2022; Fässler, 2023).

---

7 A pesar de que en este trabajo el *neurotargeting* se considera un método más de *microtargeting*, existe una diferencia notable entre el resto de los métodos de *microtargeting* y el *neurotargeting*. El resto de los métodos de *microtargeting* se basan en la extracción y explotación de datos de la ciudadanía creados de forma consciente por esta, mientras que el *neurotargeting* se cimienta en la extracción y explotación de conjuntos de datos de la intimidad corporal que no han sido creados de forma consciente por las personas.

3. El *microtargeting* político en las democracias occidentales

La capacidad del *microtargeting* político de realizar una propaganda computacional automatizada, *algoritmizada*, personalizada, e incluso sintética, permite dirigir contenidos específicos, hacia votantes específicos, en momentos específicos y vincularlos directamente con sus características intimas, sus sesgos y sus vulnerabilidades para lograr una persuasión y manipulación política máxima (Bashyakaria et al., 2019). Además de estas características, que ya de por sí adulteran los procesos democráticos y ponen en serio riesgo los principios básicos de las democracias deliberativas occidentales (Habermas, 2021), estos efectos negativos se pueden agravar a través de la difusión de contenidos ligados con informaciones de dudosa veracidad, desinformaciones, *fake news o deep fakes* (D'Ancona, 2019; Howard, 2020; Nightingale y Farid, 2022; Woolley, 2023) o por medio del bombardeo de propaganda a determinados colectivos con rasgos antisociales, impulsivos o agresivos para que estos se inflamen y creen un clima de distorsión social "(Garcia y Sikström, 2014; González Moraga, 2015; Jamieson, 2018; Wylie, 2019). Dawson (2021) resume esta situación diciendo que el *microtargeting* político:

> allows individual-level messaging to be deployed to influence voting behavior and is able to be leveraged for more insidious dis/misinformation campaigns. What started as a way for businesses to connect directly with potential customers has transformed into a disinformation machine at a scale that autocratic governments of the past could only imagine. (p.64)

Este fragmento enfatiza los principales efectos negativos y la peligrosidad del *microtargeting* político para el sistema democrático. Estas cuestiones se acrecientan como consecuencia del desconocimiento de la ciudadanía de la extracción y explotación de sus datos para la realización de *microtargeting* político y de las características de este fenómeno (Llaneza, 2019). La mayoría de los ciudadanos no tienen en consideración que los contenidos políticos a los cuales están expuestos en los ecosistemas *ciberfísicos* no son objetivos y están fuertemente influenciados y sesgados en favor de los intereses del anunciante (Fässler, 2023).

La puesta en marcha de *microtargeting* político provoca impactos negativos en los pilares fundamentales de las democracias deliberativas occidentales principalmente a través de dos ámbitos. Por una parte, la monitorización, extracción y explotación de grandes conjuntos de datos de la privacidad e intimidad de cada persona socava la integridad, la dignidad, la personalidad y el anonimato de cada persona dando lugar a la posibilidad de monitorizar sus comportamientos y controlar sus acciones y actividades (Zuboff, 2020; Han, 2021; Varoufakis, 2023). Por otra parte, la capacidad de creación de contenidos totalmente personalizados de forma automatizada y *algoritmizada* para cada individuo —basados en la explotación de los datos privados e íntimos de las personas— erosiona el conocimiento y la veracidad necesarias para el correcto funcionamiento de democracia (Woolley, 2023). La combinación de estos factores hace posible que los individuos, empresas, organizaciones o instituciones que ponen en marcha el *microtargeting* político puedan intervenir y condicionar la soberanía, autonomía y autodeterminación de la ciudadanía y producir una falta de agencia epistémica

que ponga en cuestión el control de la ciudadanía sobre la construcción de su propia ideología y sus propias convicciones políticas (Coeckelbergh, 2022, 2024).

Para hacer frente a los efectos dañinos del *microtargeting* político en los procesos democráticos de las sociedades occidentales, actualmente existen dos enfoques reglamentaritos totalmente diferentes: el de la UE y el de los EEUU.

La UE tiene una clara voluntad de regular y limitar los efectos dañinos del *microtargeting* en los sistemas democráticos y ha desarrollado un amplio paquete de regulaciones para este propósito (Galli et al., 2022; Fässler, 2023). Entre estas regulaciones destacan el GDPR (General Data Protection Regulation), la DSA (Digital Services Act) y la AIA (Artificial Intelligence Act) ya que afrontan la extracción de datos, la transparencia, la segmentación y la personalización de los anuncios políticos.

En primer lugar, el GDPR ha hecho obligatoria para cualquier organización que extraiga y explote datos la obtención de un consentimiento «valido» de las personas afectadas a la hora de extraer y usar datos privados y también introduce la posibilidad de que los ciudadanos puedan optar por limitar la explotación de sus datos privados para la realización de propaganda directa. En segundo lugar, la DSA, por una parte, obliga a las grandes plataformas digitales a evaluar los riesgos de los contenidos de sus plataformas para los procesos electorales, la seguridad pública y la desinformación y a tomar medidas para mitigarlos y a aumentar la transparencia y control en relación con la propaganda política. Por otra parte, afronta directamente los problemas del *microtargeting* político prohibiendo las técnicas de segmentación y personalización que impliquen la utilización de datos personales específicos como puedan ser datos vinculadas con la salud, la raza o las creencias religiosas. Finalmente, la AIA, por una parte, busca que el uso de la inteligencia artificial generativa en el ámbito del *microtargeting* sea transparente, ética y responsable y, por otra parte, que esta no pueda ser utilizada para socavar los derechos y libertades fundamentales de los ciudadanos y los procesos democráticos.

El tejido regulativo de la UE es uno de los más desarrollados del mundo, por no decir el más desarrollado, en materia de protección de datos, transparencia, consentimiento y lucha contra la manipulación política. A pesar de esto, la ciudadanía europea aún está expuesta a determinados riesgos que pueden socavar los procesos democráticos. Por una parte, algunas de las grandes corporaciones digitales estadounidenses, como Google, Meta y Amazon, han sido multadas y amonestadas por incumplir las prerrogativas del GDPR y de la DSA y por transferir de forma continuada grandes conjuntos de datos a EEUU para evitar las reglamentaciones de la UE (Commission Nationale de l'Informatique et des Libertés, 2022; European Data Protection Board, 2022; Perez Colome y Ayuso, 2023). Por otra parte, en las políticas de privacidad de las grandes corporaciones digitales chinas se indica que los conjuntos de datos de los europeos pueden ser trasladados y explotados fueras de las fronteras de la UE sin tener en cuenta las leyes de la UE, además de poder ser utilizados por el propio gobierno chino (Hoffman y Attrill, 2021). Por último, la prohibición de las técnicas de segmentación y personalización que impliquen la utilización de datos personales específicos plasmadas en DSA pueden ser sorteadas por medio de la obtención del consentimiento —en la mayoría de casos a través de un modo no totalmente informado— de las personas afectadas (Fässler, 2023).

En EEUU no hay ninguna regulación estatal en relación con la extracción masiva de datos, la inteligencia artificial generativa, el *microtargeting* político y los efectos que el capitalismo de la vigilancia puede causar en los procesos democráticos (Dawson, 2021, 2023) y además se está impidiendo judicialmente al gobierno realizar cualquier tipo de regulación de este tipo (Zakrzewski, 2023). En relación con los grandes conjuntos de datos, en EEUU los datos privados pueden ser extraídos, comprados, transferidos o explotados por cualquier personaje nacional o extranjero sin prácticamente limitaciones. En relación con el *microtargeting* político, existen algunas limitaciones vinculadas con la realización de propaganda política personalizada por parte de la administración y del gobierno de los EEUU, pero ninguna limitación en las técnicas, los contenidos o los objetivos del resto de actores (candidatos, partidos políticos, empresarios, poderes fácticos, gobiernos extranjeros, etc.) (Dawson, 2023). Las únicas limitaciones existentes en este caso son las débiles e interesadas autorregulaciones introducidas por algunas de las grandes corporaciones digitales fuertemente dependientes del mercado de la publicidad (Fässler, 2023).

En el caso de la UE, a pesar de los grandes esfuerzos regulativos realizados, los procesos democráticos y la ciudadanía aún se pueden ver influenciados y manipulados por el *microtargeting* político como consecuencia de, principalmente, dos cuestiones. En un primer momento, la llamada "paradoja de la privacidad" (Acquisti y Grossklags, 2005). Los ciudadanos europeos son conscientes de los riesgos de la extracción y explotación de sus datos para fines comerciales y propagandísticos, pero dan su consentimiento, para de esta forma, poder continuar utilizando las plataformas y los programas tecnológicos (Lastra-Anadón y Rubio, 2020; Solove, 2021). En un segundo momento, la transferencia de estos grandes conjuntos de datos al extranjero para poder explotarlos obviando las reglamentaciones europeas supone de facto la posibilidad de *hipersegmentar* a la ciudadanía europea, personalizar contenidos y realizar propaganda computacional automatizada y *algoritmizada* (Saura García, 2024).

La UE debe seguir desarrollando y actualizando sus regulaciones para hacer frente a los impactos negativos de la vigilancia social masiva y el *microtargeting* político sobre los sistemas democráticos provocados por la recopilación e intercambio de información y por la explotación de los sesgos y las vulnerabilidades de los ciudadanos. Para lograr este propósito, Galli et al. (2022) argumentan que se deben ampliar y desarrollar medidas específicas destinadas a garantizar el libre consentimiento en relación a la extracción y explotación de datos, limitar la posibilidad de otorgar el consentimiento para la extracción y explotación de datos a cambio de servicios y contraprestaciones y promover un ecosistema de intercambio de datos libre y justo que proteja los datos de los ciudadanos europeos.

En el caso de los EEUU, Dawson (2021) resume la situación diciendo que el ecosistema totalmente desregulado del capitalismo de la vigilancia y del *microtargeting* político estadunidense pone en serio riesgo la capacidad de opinar y reflexionar de la ciudadanía, la soberanía popular y el correcto funcionamiento de la democracia en nombre del libre mercado económico. De la misma forma, también aumenta desmesuradamente el poder económico y político de terceros actores, como son poderes facticos, gobiernos extranjeros, personajes multimillonarios, etc. (Da Empoli, 2020; Zuboff, 2020).

4. Conclusiones

La vigilancia, control y manipulación política de la ciudadanía a través de la extracción y explotación de sus datos y metadatos personales y de campañas de manipulación política automatizadas y *algoritmizadas*, entre las que destaca el *microtargeting,* pero también las cámaras de resonancia, los filtros de burbuja o la utilización masiva de *bots*, crean una opinión pública artificial y sintética y ponen en serio riesgo el correcto funcionamiento de los procesos y los sistemas democráticos en general (García-Marzá y Calvo, 2022, 2024).

El desarrollo exponencial de las técnicas, por una parte, de *datificación* y extracción de datos y metadatos y, por otra parte, de manipulación política en diferentes frentes, como son los *deep fakes*, la tecnología *deep learning* y el uso de inteligencia artificial generativa a un ritmo mucho más rápido que el de cualquier posible actualización de la regulación (Helmus, 2022; Millière, 2022), el incumplimiento de la reglamentación existente por parte de algunas de las corporaciones digitales más importantes del mundo (Saura García, 2024) y la indiferencia radical del modelo de negocio del capitalismo de la vigilancia por la libertad de expresión y los pilares de los sistemas democráticos (Zuboff, 2020) están transformando el actual formato democrático en una democracia de la vigilancia de carácter artificial, sintético, instrumental, sesgado y despótico.

La democracia de la vigilancia hace referencia a un formato democrático emergente en el que los procesos implicados quedan desvirtuados y vaciados de legitimidad como consecuencia del contexto de vigilancia, control y manipulación política que limita la capacidad de opinar y reflexionar de la ciudadanía por medio de la personalización, artificialización y sintetificación de la información que consume la ciudadanía y la destrucción de la opinión pública crítica y madura (Saura García, 2023; Calvo y Saura García, en prensa). El funcionamiento de la democracia de la vigilancia mantiene todo el poder de la democracia en la ciudadanía, pero de forma instrumental, puesto que la extracción de datos y la propaganda computacional política provocan que estos sean unas marionetas de los intereses políticos de las grandes corporaciones digitales, los poderes fácticos, los personajes multimillonarios o los gobiernos extranjeros.

Bibliografía

Acquisti, A., y Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy*, *3*(1), 26-33. https://doi.org/10.1109/MSP.2005.22

Armenteras, D., González, T. M., Vergara, L. K., Luque, F. J., Rodríguez, N., y Bonilla, M. A. (2016). A review of the ecosystem concept as a "unit of nature" 80 years after its formulation. *Ecosistemas*, *25*(1), 83-89. https://doi.org/10.7818/ECOS.2016.25-1.12

Bakir, V. (2020). Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting. *Frontiers in Communication*, *5*(67), 1-16. https://doi.org/10.3389/fcomm.2020.00067

Bartlett, J., Smith, J., y Acton, R. (2018). *The Future of Political Campaigning*. Demos. Recuperado de https://ico.org.uk/media/2259365/the-future-of-political-campaigning.pdf

Bashyakaria, V., Hankey, S., Macintyre, A., Renno, R., y Wright, G. (2019). *Personal Data: Political Persuasion Inside the Influence Industry. How it works.* Tactical Tech's Data

and Politics. Recuperado de https://cdn.ttc.io/s/tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works.pdf

Bimber, B. (2014). Digital Media in the Obama Campaigns of 2008 and 2012: Adaptation to the Personalized Political Communication Environment. *Journal of Information Technology & Politics*, *11*(2), 130-150. https://doi.org/10.1080/19331681.2014.895691

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

Cadwalladr, C. (14 de mayo de 2017). Follow the data: does a legal document link Brexit campaigns to US billionaire?. *The Guardian*. Recuperado de https://www.theguardian.com/technology/2017/may/14/robert-mercer-cambridge-analytica-leave-eu-referendum-brexit-campaigns

Calvo, P. (2019). Democracia algorítmica: consideraciones éticas sobre la dataficación de la esfera pública. *Revista del Clad. Reforma y Democracia*, *74*, 5-30.

Calvo, P. (2020). Democracia aumentada. Un ecosistema ciberético para una participación política basada en algoritmos. *Ápeiron. Estudios de Filosofía*, *12*, 129-141.

Calvo, P. (2021). El gobierno ético de los datos masivos. *Dilemata*, *34*, 31-49.

Calvo, P. y Saura García C. (en prensa). Democracia de la vigilancia: datos, activismo y contrapoder. *Revista Internacional de Pensamiento Político*, 19.

Coeckelbergh, M. (2022). Democracy, epistemic agency, and AI: political epistemology in times of artificial intelligence. *AI and Ethics*, *3*(4), 1341-1350. https://doi.org/10.1007/S43681-022-00239-4

Coeckelbergh, M. (2024). *Why AI Undermines Democracy and What To Do About It*. Cambridge: Polity Press.

Commission Nationale de l'Informatique et des Libertés. (2022). Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply. Recuperado de https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply

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

Da Empoli, G. (2020). *Los ingenieros del caos*. Madrid: Ediciones Anaya.

Dawson, J. (2021). Microtargeting as Information Warfare. *The Cyber Defense Review*, *6*(1), 63-80. https://doi.org/10.2307/26994113

Dawson, J. (2023). Who Controls the Code, Controls the System: Algorithmically Amplified Bullshit, Social Inequality, and the Ubiquitous Surveillance of Everyday Life. *Sociological Forum*, 1-24. https://doi.org/10.1111/SOCF.12907

De Miguel, R. (17 de junio de 2024). Cámaras con IA en el metro de Londres captan el estado emocional de los viajeros. *El País*. Recuperado de https://elpais.com/ciencia/2024-06-17/camaras-con-ia-en-el-metro-de-londres-captan-el-estado-emocional-de-los-viajeros.html

Deibert, R. J. (2019). The Road to Digital Unfreedom: Three Painful Truths About Social Media. *Journal of Democracy*, *30*(1), 25-39. https://doi.org/10.1353/JOD.2019.0002

Ebeling, M. F. E. (2022). *Afterlives of data : life and debt under capitalist surveillance*. Berkeley: University of California Press.

European Data Protection Board. (2022). Italian SA bans use of Google Analytics: no adequate safeguards for data transfers from Caffeina Media S.r.l. to the U.S. Recuperado de https://edpb.europa.eu/news/national-news/2022/italian-sa-bans-use-google-analytics-no-adequate-safeguards-data-transfers_en

Farahany, N. A. (2023). *The Battle for Your Brain*. New York: St. Martin's Press.

Fässler, M. (2023). *Google's Privacy Sandbox Initiative: Old wine in new skins* (N.º 2023/01). Recuperado de https://www.zora.uzh.ch/id/eprint/232978/1/Google_s_Privacy_Sandbox.pdf

Fowler, G. A. (6 de septiembre de 2022a). Your kids' apps are spying on them. *The Washington Post*. Recuperado de https://www.washingtonpost.com/technology/2022/06/09/apps-kids-privacy/

Fowler, G. A. (12 de octubre de 2022b). Tour Amazon's dream home, where every appliance is also a spy. *The Washington Post*. Recuperado de https://www.washingtonpost.com/technology/interactive/2022/amazon-smart-home/

Galli, F. (2021). *Algorithmic business and EU law on fair trading*. Università di Bologna. Recuperado de http://amsdottorato.unibo.it/9750/1/tesifinale_galli.pdf

Galli, F., Lagioia, F., y Sartor, G. (2022). Consent to Targeted Advertising. *European Business Law Review*, *33*(4), 485-512. https://doi.org/10.54648/EULR2022023

García-Marzá, D., y Calvo, P. (2022). Democracia algorítmica: ¿un nuevo cambio estructural de la opinión pública? *Isegoría*, (67), e17. https://doi.org/10.3989/ISEGORIA.2022.67.17

García-Marzá, D., y Calvo, P. (2024). *Algorithmic democracy: A critical perspective from deliberative democracy*. Cham: Springer.

Garcia, D., y Sikström, S. (2014). The dark side of Facebook: Semantic representations of status updates predict the Dark Triad of personality. *Personality and Individual Differences*, *67*, 69-74. https://doi.org/10.1016/j.paid.2013.10.001

Gerber, A. S., Huber, G. A., Doherty, D., y Dowling, C. M. (2011). The Big Five Personality Traits in the Political Arena. *Annual Review of Political Science*, *14*, 265-287. https://doi.org/10.1146/ANNUREV-POLISCI-051010-111659

Gerodimos, R., y Justinussen, J. (2015). Obama's 2012 Facebook Campaign: Political Communication in the Age of the Like Button. *Journal of Information Technology & Politics*, *12*(2), 113-132. https://doi.org/10.1080/19331681.2014.982266

González Moraga, F. R. (2015). La tríada oscura de la personalidad: maquiavelismo, narcisismo y psicopatía. *Revista Criminalidad*, *57*(2), 253-265. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=5456799

Habermas, J. (2021). Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit. En M. Seelinger & S. Sevignani (Eds.), *Ein neuer Strukturwandel der Öffentlichkeit?* (pp. 470-500). Baden-Baden: Nomos.

Haig, Z., y Hajdu, V. (2017). New Ways in the Cognitive Dimension of Information Operations. *Land Forces Academy Review*, *22*(2), 94-102. https://doi.org/10.1515/raft-2017-0013

Han, B. C. (2021). *Psicopolítica: Neoliberalismo y nuevas técnicas de poder*. Barcelona: Herder.

Helmus, T. C. (2022). *Artificial Intelligence, Deepfakes, and Disinformation*. RAND Corporation. https://doi.org/10.7249/PEA1043-1

Hersh, E. D. (2015). *Hacking the Electorate: How Campaigns Perceive Voters* . Cambridge: Cambridge University Press.

Hoffman, S., y Attrill, N. (2021). *Mapping China's Tech Giants: Supply chains and the global data collection ecosystem* (N.º 45/2021). The Australian Strategic Policy Institute. Recuperado de https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2021-06/Supply chains.pdf?VersionId=56J_tt8xYXYvsMuhriQt5dSsr92ADaZH

Howard, P. N. (2020). *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*. New Haven: Yale Univeristy Press.

Issenberg, S. (2012). *The victory lab: the secret science of winning campaigns*. New York: Broadway Books.

Iyer, P., Riedl, M. J., Trauthig, I. K., y Woolley, S. (2021). *Location-based targeting: history, usage, and related concerns*. University of Texas at Austin. Center for Media Engagement. Recuperado de https://mediaengagement.org/research/location-based-targeting-history-usage-and-related-concerns/

Jamieson, K. H. (2018). *Cyberwar: How Russian hackers and trolls helped elect a president: What we don't, can't, and do know*. Oxford: Oxford University Press.

Juárez Ramos, V. (2019). *Analyzing the Role of Cognitive Biases in the Decision-Making Process*. Hershey: IGI Global.

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

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

Kosinski, M. (2021). Facial recognition technology can expose political orientation from naturalistic facial images. *Scientific Reports*, *11*(1), 100. https://doi.org/10.1038/s41598-020-79310-1

Kosinski, M., Stillwell, D., y Graepel, T. (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

Lastra-Anadón, C., y Rubio, D. (2020). *European Tech Insights 2020*. IE Center for the Governance of Change (CGC). Recuperado de https://docs.ie.edu/cgc/CGC-European-Tech-Insights-2020.pdf

Llaneza, P. (2019). *Datanomics: Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos*. Barcelona: Deusto.

Matz, S. C., Kosinski, M., Nave, G., y Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences of the United States of America*, *114*(48), 12714-12719. https://doi.org/10.1073/PNAS.1710966114/SUPPL_FILE/PNAS.1710966114.SAPP.PDF

Mayer-Schönberger, V., y Cukier, K. (2013). *Big data: La revolución de los datos masivos*. Madrid: Turner Publicaciones.

Mercier, H., y Sperber, D. (2017). *The Enigma of Reason*. Cambridge: Harvard University Press.

Millière, R. (2022). Deep learning and synthetic media. *Synthese*, *200*(3), 1-27. https://doi.org/10.1007/S11229-022-03739-2/FIGURES/6

Moriyama, T. (2022). *Empire of Direct Mail: How Conservative Marketing Persuaded Voters and Transformed the Grassroots*. Kansas: University Press of Kansas

Nave, G., Greenberg, D. M., Kosinski, M., Stillwell, D., y Rentfrow, J. (2018). Musical Preferences Predict Personality: Evidence from Active Listening and Facebook Likes. *Pyschological Science*, *29*(7), 1145-1158. https://doi.org/10.1177/0956797618761659

Nightingale, S. J., y Farid, H. (2022). AI-synthesized faces are indistinguishable from real faces and more trustworthy. *Proceedings of the National Academy of Sciences of the United States of America*, *119*(8), e2120481119. https://doi.org/10.1073/PNAS.2120481119/ASSET/E74865F1-3BC4-4BEC-8325-DEB222AE2CB4/ASSETS/IMAGES/LARGE/PNAS.2120481119FIG04.JPG

Perez Colome, J., y Ayuso, S. (22 de mayo de 2023). Irlanda impone a Meta una multa de 1.200 millones de euros, la mayor sanción europea por infracción de privacidad. *El País*. Recuperado de https://elpais.com/tecnologia/2023-05-22/irlanda-impone-a-meta-una-multa-de-1200-millones-de-euros-la-mayor-sancion-europea-por-infraccion-de-privacidad.html

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

Sanborn, F. W., y Harris, R. J. (2018). *A cognitive psychology of mass communication*. New York: Routledge.

Saura García, C. (2023). El big data en los procesos políticos: hacia una democracia de la vigilancia. *Revista de filosofía*, *80*, 215-232. https://doi.org/10.4067/S0718-43602023000100215

Saura García, C. (2024). Digital expansionism and big tech companies: consequences in democracies of the European Union. *Humanities and Social Sciences Communications*, *11*(448), 1-8. https://doi.org/10.1057/s41599-024-02924-7

Schick, N. (2020). *Deep Fakes and the Infocalypse : What You Urgently Need To Know*. London: Monorary.

Schumpeter, J. A. (1958). *Capitalismo, socialismo y democracia*. Madrid : Aguilar.

Singer, N. (15 de septiembre de 2022). This Ad's for You (Not Your Neighbor). *The New York Times*. Recuperado de https://www.nytimes.com/2022/09/15/business/custom-political-ads.html

Solove, D. J. (2021). The Myth of the Privacy Paradox. *George Washington Law Review*, *89*(1), 1-51. https://doi.org/10.2139/SSRN.3536265

Thompson, S. A., y Warzel, C. (19 de diciembre de 2019). Twelve Million Phones, One Dataset, Zero Privacy. *The New York Times*. Recuperado de https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

Turow, J. (2021). *The voice catchers : how marketers listen in to exploit your feelings, your privacy, and your wallet*. New Haven: Yale University Press.

Varoufakis, Y. (2023). *Technofeudalism: What Killed Capitalism*. London: Random House.

Woolley, S. (2023). *Manufacturing consensus : understanding propaganda in the era of automation and anonymity*. New Haven: Yale University Press.

Woolley, S., y Gursky, J. (21 de junio de 2020). The Trump 2020 app is a voter surveillance tool of extraordinary power. *MIT Technology Review*. Recuperado de https://www.technologyreview.com/2020/06/21/1004228/trumps-data-hungry-invasive-app-is-a-voter-surveillance-tool-of-extraordinary-scope/

Woolley, S., & Howard, P. N. (Eds.). (2018). *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford: Oxford University Press.

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

Youyou, W., Kosinski, M., y Stillwell, D. (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

Zakrzewski, C. (4 de julio de 2023). Judge blocks U.S. officials from tech contacts in First Amendment case. *The Washington Post*. Recuperado de https://www.msn.com/en-us/news/politics/judge-blocks-us-officials-from-tech-contacts-in-first-amendment-case/ar-AA1dq6Cj

Zewe, A. (17 de enero de 2020). Imperiled information: Students find website data leaks pose greater risks than most people realize. *Harvard John A. Paulson School of Engineering and Applied Sciences*. Recuperado de https://seas.harvard.edu/news/2020/01/imperiled-information

Zuboff, S. (2020). *La era del capitalismo de la vigilancia: la lucha por un futuro humano frente a las nuevas fronteras del poder*. Barcelona: Paidós.