Revista Española de Derecho Europeo
94 | Abril – Junio 2025
pp. 31-77
Madrid, 2025
DOI:10.37417/REDE/num94_2025_3075
© Marcial Pons Ediciones Jurídicas y Sociales
© Covadonga Ferrer Martín de Vidales
ISSN: 1579-6302
Recibido: 13/05/2025 | Aceptado: 09/06/2025

MICROTARGETING ELECTORAL: CÓMO PROTEGER LOS DATOS DE LAS OPINIONES POLÍTICAS DE LAS PERSONAS Y LUCHAR CONTRA LA DESINFORMACIÓN A TRAVÉS DE LA NORMATIVA EUROPEA

ELECTORAL MICROTARGETING: HOW TO PROTECT DATA FROM PEOPLE'S POLITICAL OPINIONS AND FIGHT DISINFORMATION THROUGH EU LEGISLATION

Covadonga Ferrer Martín de Vidales*

RESUMEN: El uso creciente de datos personales obtenidos a través de redes sociales para la distribución de propaganda electoral personalizada, mediante técnicas de *microtargeting*, se ha intensificado y sofisticado técnicamente en los últimos años. Esta práctica, combinada con la proliferación de información falsa y estrategias sistemáticas de difusión de desinformación, está generando un impacto significativo en diversos procesos electorales a nivel global, comprometiendo principios fundamentales que deben regir toda contienda electoral. Por ello, se vuelve cada vez más urgente proteger los datos personales de los usuarios, en particular aquellos vinculados a sus opiniones políticas, y combatir su uso indebido con fines de manipulación y propagación de desinformación. Este trabajo tiene como objetivo, a partir de un análisis del funcionamiento del *microtargeting* electoral

* Profesora Contratada Doctora de Derecho Constitucional, Facultad de Derecho, Universidad Complutense de Madrid, cferrerm@ucm.es, ORCID 0000-0002-8571-3012. El presente trabajo ha sido realizado en el marco del proyecto «Fortalecimiento de la Democracia y el Estado de Derecho a través de la Inteligencia Artificial», financiado por el Ministerio de Ciencia e Innovación en la Convocatoria de 2021 (Proyecto PID2021-122677NB-I00 AIDEROL).

y del impacto de la desinformación en los procesos electorales y en los derechos fundamentales, examinar si una serie de Reglamentos adoptados recientemente en el ámbito de la Unión Europea pueden contribuir a una mejor protección de estos datos y a una lucha más eficaz contra la difusión de desinformación.

PALABRAS CLAVE: *microtargeting* electoral; protección de datos; derechos fundamentales; elecciones.

ABSTRACT: The growing practice of using personal data from social networks for targeted election propaganda, alongside the spread of false information, has become more sophisticated, impacting electoral processes globally. Protecting users' personal beliefs in particular the ones regarding their political beliefs, and addressing the misuse of such data for personalised propaganda and disinformation dissemination has become increasingly crucial. This paper discusses the rise of electoral microtargeting techniques and the effects of disinformation dissemination on electoral processes and fundamental rights. It explores whether recent EU regulations can enhance the protection of such data and combat disinformation effectively. Considering these developments, the need to safeguard personal data and ensure fair electoral practices is emphasised, given the significant implications for democratic principles.

KEYWORDS: Electoral microtargeting; data protection; fundamental rights; elections.

SUMARIO: INTRODUCCIÓN.— 1. PRÁCTICAS DE *MICROTARGETING* ELECTORAL: COMO SE ELABORAN PERFILES.— 2. BURBUJAS DE FILTRO: COMO SE ESTÁ RESTRINGIENDO LA INFORMACIÓN QUE CONSULTAMOS A TRAVÉS DE LAS REDES.— 3. LOS EFECTOS DEL USO DE TÉCNICAS DE *MICROTARGETING* PARA LA DIFUSIÓN DE DESINFORMACIÓN EN PROCESOS ELECTORALES Y EN LOS DERECHOS FUNDAMENTALES. 4.— NORMATIVA EUROPEA APLICABLE A LAS TÉCNICAS DE *MICROTARGETING* ELECTORAL: 4.1. El RGPD; 4.2. El Reglamento de Transparencia y Segmentación de la publicidad política; 4.3. Otras normas de la UE que se pueden aplicar a las prácticas de *microtargeting* electoral. 4.3.1 El Reglamento de Inteligencia Artificial. 4.3.2. Los Reglamentos de Servicios y Mercados Digitales.— CONCLUSIONES.— BIBLIOGRAFÍA

INTRODUCCIÓN

Es indudable que las nuevas tecnologías han facilitado muchos aspectos de nuestra vida diaria y que presentan grandes ventajas[1]. Internet ha dado

[1] Como señala la Comisión de Venecia, las nuevas tecnologías y las redes sociales han revolucionado la forma en que la gente interactúa y ejerce sus derechos a la libertad de expresión e información, por ejemplo, para demandar mejores servicios, más transparencia o una participación más significativa en la esfera política. European

un acceso sin precedentes a los ciudadanos a todo tipo de información y, en concreto, a la información electoral, permitiéndoles expresar sus opiniones e involucrarse activamente en las campañas electorales[2]. También es una plataforma útil para que los partidos presenten sus programas al electorado y tratar de movilizar así un mayor apoyo[3].

Las nuevas tecnologías y las redes sociales también permiten en la actualidad elaborar perfiles de forma mucho más precisa, a través de los datos que se obtienen de las páginas web que visitamos, nuestras redes sociales, y las compras que realizamos. Esto permite el envío de propaganda o publicidad personalizada, adecuada a los gustos del grupo al que va dirigida, con el objetivo de aumentar las posibilidades de que realicen una determinada acción. Se trata de una potencialidad a la que no han sido ajenos los partidos políticos, que tienen un interés cada vez más creciente en dichos datos[4].

Puede que no se trate de algo novedoso pues, como señalan Rosario García Mahamut y Mónica Arenas Ramiro, es habitual que los partidos adapten sus mensajes al público y tengan en cuenta sus intereses específicos para conseguir el mayor número de votos posibles y que, por lo tanto, traten de utilizar los datos personales de los electores de forma que puedan llegar a ellos de una manera más personalizada, aumentando las posibilidades de conseguir así su voto[5].

Si se realiza un uso correcto de esos datos y de las técnicas de *microtargeting* pueden lograrse buenos resultados, como ya demostró la campaña que llevó a Obama a la presidencia[6]. Ahora bien, la combinación de las técnicas de *microtargeting* con la difusión de desinformación para influir en los resultados electorales está poniendo actualmente en riesgo nuestros modelos de democracia. Ya en el año 2016, el escándalo de Cambridge Analytica, que adquirió de forma indebida de Facebook los datos de millones de usuarios

---

Commission for Democracy through Law (Venice Commission), *Joint Report of the Venice Commission and of the Directorate of Information Society and Action against crime of the Directorate General of Human Rights and Rule of Law (DGI) on Digital Technologies and Elections*, adopted by the Venice Commission at its 119th Plenary Session (Venice, 21-22 June 2019) CDL-AD (2019)016 (En adelante, Joint Report of the Venice Commission on Digital Technologies and Elections): apdo. 4, p. 3. Disponible en *https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2019)016-e*

[2] Council of Europe, *Internet and electoral campaigns. Study on the use of Internet in electoral campaigns*. DGI (2017)11: 7.

[3] *Ibid.*

[4] Mónica Arenas Ramiro, «Partidos políticos, opiniones políticas e Internet: la lesión del derecho a la protección de datos personales», *Teoría y Realidad Constitucional*, núm. 44 (2019): 342, *doi.org/10.5944/trc.44.2019.26005*.

[5] Rosario García Mahamut, «Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español», *Teoría y Realidad Constitucional* núm. 35 (2015): 309-310, 320 y ss, *doi.org/10.5944/trc.35.2015.14921*; Arenas Ramiro, «Partidos políticos», 342.

[6] Más información sobre las dos campañas de Obama en Ludwig Huber, *Democracia 2.0: El poder político en la era digital*, IEP, Perú (2023): 1919 y ss.

de la red que fueron utilizados para influir posteriormente —mediante técnicas de *microtargeting*[7]— en las opiniones de los votantes, es una buena muestra de los efectos e influencia que estas prácticas pueden tener en unas elecciones[8].

La proliferación de información falsa y de tácticas de desinformación, tanto desde actores públicos como privados, se ha extendido y se ha vuelto más sofisticada técnicamente en los últimos años[9], y preocupa asimismo la intervención extranjera en las elecciones de otros países como método para desestabilizar las democracias[10]. Las nuevas tecnologías posibilitan la monitorización de las actividades que se realizan en la red y la manipulación del comportamiento, amenazando de esta forma como señala la Comisión de Venecia «la autenticidad del sufragio, la equidad de los procesos electorales y, de forma ulterior, la capacidad de traducir el *deseo del pueblo* en representa-

---

[7] Como señala Luis Miguel González de la Garza, mediante estas técnicas se agrupa a los electores en segmentos pequeños o *clusters* que se sincronizan con perfiles psicométricos ya elaborados, para enviar así propaganda electoral personalizada. El *microtargeting* electoral aprende del elector y le ofrecerá «variantes de campaña propagandística adaptadas a su perfil ideológico». Luis Miguel González De La Garza, «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* nº 103 (septiembre-diciembre 2018): 283 y ss, *doi.org/10.5944/rdp.103.2018.23203*.

[8] *Ibid.* Como señalan Pérez-Escolar y Alcaide-Pulido, el uso de la técnica de *microtargeting* se pervierte cuando se utiliza para agrupar a los ciudadanos en «microcomunidades o nichos radicales con opiniones opuestas» y, de esta forma, aumentar la polarización o incitar a la supresión del voto. Marta Pérez-Escolar y Purificación Alcaide-Pulido, «La polarización ideológica y la desinformación como estrategias propagandísticas en la guerra híbrida» en *Desinformación y Defensa. Conflictos híbridos, entorno cognitivo y operaciones de influencia*, Juan Miguel Aguado y otros (Madrid: Dykinson, 2024), 81. Un análisis no solo del caso de Cambridge analítica, sino también del gran poder de influencia en las democracias y procesos electorales que tienen las cyber operaciones basadas en grandes bases de datos, en Dominik Steiger, «International law and new challenges to democracy in the digital age. Big data, privacy and interverences with the political process» in Big *Data, Political Campaigning and the Law. Democracy and Privacy in the age of micro-targeting*, edited by Normann Witzledb, Moira Paterson and Janice Richardson, (New York: Routledge, 2020): 71-98.

[9] Como señala María Garrote de Marcos, los nuevos contenidos generados con IA hacen que la desinformación sea más convincente y, no solo es más fácil de crear, sino que cada vez es más difícil de detectar y contrarrestar. María Garrote de Marcos, «La IA en el período electoral: tres propuestas a partir de la integridad electoral» en *Fortalecimiento de la democracia y el Estado de Derecho a través de la inteligencia artificial*, ed. por Rafael Bustos Gisbert, Javier García Roca (Oñati: IVAP, 2025): 264.

[10] *Joint Report of the Venice Commission on Digital Technologies and Elections*, apdos. 16 y 17. Por ello, distintos países están aprobando normativas para combatir el uso de información falsa durante las campañas electorales y obligar a que dichos contenidos se eliminen lo más rápidamente posible. En el informe de la Comisión de Venecia de 2019 pueden consultarse las distintas normativas e iniciativas adoptadas a nivel nacional. *Ibid.* apdos. 99 y ss. Las normas adoptadas desde la UE que permitirán combatir también este problema se examinarán más adelante en el presente trabajo.

ción institucional y decisiones de gobierno»[11]. Los principios de objetividad, neutralidad política, transparencia e igualdad de armas que deben garantizar toda competición electoral, como destaca Rosario García Mahamut, pueden verse afectados cuando se hace un uso indebido de los datos obtenidos a través de las nuevas tecnologías con el objetivo de «construir alternativas de poder lejos de la defensa del interés general» y de atacar las reglas del juego democrático que garantizan la alternancia[12], como ocurrió en las elecciones de EEUU en 2016, en las de 2019 con las acusaciones e intentos de Donald Trump de sembrar dudas sobre la validez de los resultados a través de las redes sociales[13], y en las últimas elecciones de 2024 en las que finalmente Trump ha conseguido volver a la presidencia[14].

El presente trabajo tiene por objeto examinar cómo se pueden proteger los datos personales de los usuarios, en particular los relativos a sus opiniones políticas, y luchar contra la desinformación a través de la normativa europea. A dichos efectos, en primer lugar, es necesario entender en qué consisten las prácticas de *microtargeting* electoral y cómo se pueden elaborar perfiles ideológicos de las personas, así como cómo los sistemas de recomendaciones que se utilizan en las redes sociales y otras plataformas están limitando cada vez más la diversidad de información a la que accedemos, contribuyendo a la polarización de la sociedad e influyendo en los procesos electorales, lo que tiene efectos sobre los derechos fundamentales consagrados constitucionalmente. Realizado dicho análisis, en segundo lugar, se pasará a examinar si la actual normativa a nivel de la Unión Europea puede contribuir a poner límite a la utilización de prácticas de *microtargeting* electoral para la difusión de desinformación, así como reforzar la protección de los datos de los usuarios, evitando que se utilicen de forma abusiva por este tipo de prácticas. Por último, se tratará de concluir con algunas propuestas que puedan contribuir a aportar soluciones a la problemática examinada.

---

[11] *Ibid.* apdos. 35-36.

[12] García Mahamut, «Partidos políticos y derecho a la protección de datos», 309-310.

[13] Amanda Mars, «Trump acusa sin pruebas a Biden de querer "robar" las elecciones con "votos ilegales"», *El País*, 6 de noviembre de 2020, acceso el 10 de febrero de 2025, *https://elpais.com/internacional/elecciones-usa/2020-11-06/trump-acusa-sin-pruebas-a-biden-de-querer-robar-las-elecciones-con-votos-ilegales.html*

[14] Puede observarse cómo este ha sido un elemento destacado por distintos medios de comunicación durante la campaña electoral Blanca Bayo Pérez, «Elecciones EE.UU. 2024. El uso de la IA como herramienta de desinformación en la campaña», *El País*, 3 de noviembre de 2024, acceso el 10 de febrero de 2025, *https://www.rtve.es/noticias/20241103/elecciones-eeuu-2024-ia-herramienta-desinformacion-campana/16307898.shtml*; Daniel Iriarte, «Todo lo que Elon Musk está haciendo para que Trump gane las elecciones», *El Confidencial*, 24 de octubre de 2024, acceso el 11 de febrero de 2025, *https://www.elconfidencial.com/mundo/2024-10-24/elon-musk-campana-trump-elecciones-eeuu_3989361/*; Sarah Steffen, «Fact check: Disinformation's impact on the US election», *DW*, 11 de julio de 2024, acceso el 11 de febrero de 2025, *https://www.dw.com/en/fact-check-what-role-did-disinformation-play-in-the-us-election/a-70729575*.

1. PRÁCTICAS DE MICROTARGETING ELECTORAL: COMO SE ELABORAN PERFILES

Como se ha adelantado, actualmente los partidos políticos hacen uso de las redes sociales no solo para tratar de llegar a un mayor número de posibles votantes sino porque, a través de las herramientas de que disponen dichas plataformas para recoger los datos de los usuarios y clasificar y segmentar las preferencias de estos, pueden adecuar sus mensajes al perfil de grupos específicos[15].

Se trata del fenómeno llamado *microtargeting*, que a través de la minería de datos y la combinación de múltiples bases de datos posibilita la realización de análisis predictivos[16]. Es decir, aplicando a los datos recopilados técnicas como las que se explican en el siguiente apartado, se tratará de predecir las preferencias del usuario para, en una siguiente fase, enviar la propaganda personalizada[17]. No es que se trate de una técnica novedosa, utilizada solo por los partidos políticos. Su uso es habitual en el ámbito de la publicidad online y las técnicas empleadas son las mismas[18].

Ahora bien, como señalan Richardson, Witzleb y Paterson el uso de estas técnicas plantea una serie de cuestiones íntimamente ligadas con el núcleo central de los sistemas de gobierno democráticos como, por ejemplo, hasta qué punto estas prácticas conllevan técnicas de manipulación inaceptables o si el uso de mensajes personalizados está exacerbando la cuestión de los filtros burbuja —que se examina en el siguiente apartado—, lo que a su vez puede socavar «algunos de los procesos inherentemente colectivos que sustentan la gobernanza democrática»[19].

---

[15] Cristina Blasi Casagra y Mathias Vermueulen, «Reflections on the murky legal practices of political micro-targeting from a GDPR perspective», *International Data Privacy Law*, Vol 11, No 4 (2021): 348, *doi.org/10.1093/idpl/ipab018*.

[16] Para ello, se seleccionan grupos pequeños y homogéneos, con características comunes. *Ibid.*

[17] Pueden aplicarse diversos métodos a estas prácticas de *microtargeting*, para lograr la mayor personalización, como el *geotargeting*, el *psicotargeting*, el *targeting cognitivo*, el *A/B testing*, o el *neurotargeting*. Carlos Saura García, «Microtargeting político y vigilancia social masiva: impactos negativos en las democracias occidentales», *Daimon. Revista Internacional de Filosofía*, nº 93 (Septiembre-Diciembre 2024): 78 y ss, *doi.org/10.6018/daimon.609851*.

[18] Una sencilla explicación de cómo utilizar las técnicas de *microtargeting* en publicidad en Rubén Ortiz, «Cómo hacer *microtargeting* con publicidad digital», *SEOCOM*, 4 de diciembre de 2024, acceso el 17 de febrero de 2025, *https://seocom.agency/blog/como-hacer-microtargeting-con-nuestra-publicidad/*.

[19] Janice Richardson; Norman Witzleb y Moira Paterson, «Political micro-targeting» en *Big Data, Political Campaigning and the Law. Democracy and Privacy in the age of micro-targeting*. Edited by Normann Witzledb, Moira Paterson and Janice Richardson (New York: Routledge, 2020): 4.

La mayoría de las redes sociales permiten que los anunciantes puedan especificar qué grupos tienen por objetivo, que tendrán más probabilidades de interesarse por ese anuncio, y a los que entonces la plataforma enviará estos. Para ello, pueden utilizarse herramientas de segmentación de audiencias basadas en atributos. Así, por ejemplo, Meta ofrece tres modelos de segmentación de audiencias[20]:

— Audiencias básicas, mediante las que se define la audiencia a quien se quiere dirigir la publicidad, utilizando criterios como la edad, los intereses, la región geográfica, etc.

— Audiencias personalizadas, para poder volver a contactar con las personas que ya hayan tenido algún contacto con la empresa, partido, etc., es decir, personas que por ejemplo ya hayan visitado un sitio web, o listas de contactos que ya tenga el partido[21].

— Audiencias similares, en las que se configura una audiencia de origen con miembros ya conocidos a efectos de que los anuncios lleguen a las personas que comparten con ellos intereses y características.

Por lo tanto, un partido político puede definir su audiencia por sexo y edad de los destinatarios, o su lugar de residencia, teniendo en cuenta sus intereses en temas como inmigración, empleo, etc., ya que todo este tipo de datos los tienen las propias redes sociales[22]. De esta forma, como ya se ha adelantado, pueden realizar una publicidad más personalizada y tratar de captar así el voto de esos ciudadanos[23].

En este caso, es la plataforma la que controla los datos y el cliente, por ejemplo, un partido político, no tendrá acceso a la información personal de los usuarios de la plataforma[24]. Lo único que puede hacer es utilizar esos datos y segmentar sus anuncios para que llegue a las personas con más probabilidades de que les voten. Ahora bien, además de los datos que los partidos pueden tener procedentes de sus miembros o contactos regulares, ha de tenerse en cuenta que también suelen acudir a empresas de análisis especializa-

---

[20] «Segmentación de anuncios. Consigue que tus anuncios lleguen a personas a las que les encantará tu empresa», Meta, acceso el 16 de diciembre de 2022, *https://es-es.facebook.com/business/ads/ad-targeting*; «¿Cómo usar audiencias personalizadas o similares?», Meta, acceso el 14 de marzo de 2023, *https://es-es.facebook.com/business/help/572877736078838?id=176276233019487*.

[21] Y, a través de los datos que posee el partido, se pueden identificar otras redes sociales del contacto existente. Blasi Casagra y Vermueulen, «Reflections on the murky legal practices», 350.

[22] Como señala Saura, el *microtargeting* político puede «crear una multitud de variables de un mismo contenido», y actualizar y optimizar esas variables en función de la ubicación geográfica de la persona o de sus rasgos psicológicos. Saura García, «Microtargeting político», 80.

[23] Pues este tipo de propaganda busca explotar los sesgos y debilidades de las personas para persuadirlas y que cambien su voto. *Ibid.* p. 81.

[24] Blasi Casagra y Vermueulen, «Reflections on the murky legal practices», 349.

das que combinan las listas que tengan los partidos con otras bases de datos para crear ficheros de votantes mejorados[25]. Además, aunque técnicamente las categorías de datos que se utilizan no revelan las opiniones políticas de los usuarios, al combinar la información que se obtiene de las redes sociales (por ejemplo, en cuestiones como educación, economía, seguridad, etc.) si se puede conocer, aunque sea de modo indirecto, la ideología de un usuario[26].

Por otra parte, hay también disponibles en el mercado herramientas que permiten ver la eficacia que están teniendo los anuncios y, en su caso, volver a segmentar los mismos, es decir, refinarlos. Es el caso de *Píxels* de Meta, que permite asegurarse de que los anuncios se están mostrando a las personas «más propensas a realizar una acción», obtener información del tráfico que se genera en el sitio web, mostrar a los visitantes del sitio los productos que han visto en este u otros productos similares, y medir las conversiones en distintos dispositivos[27].

El principal problema cuando se trata de *microtargeting* electoral y de la elaboración de perfiles con las opiniones políticas de las personas es el posible uso indebido que se haga de los mismos para tratar de influir en unas elecciones, la proliferación de información falsa y tácticas de desinformación[28], en suma, su utilización para tratar de modificar el comportamiento de los electores, lo que puede afectar gravemente a los principios que deben regir toda campaña electoral[29]. Porque, como se examina en el siguiente apartado, la información que consultamos cada vez es más restringida, por lo que no se fomenta el pluralismo que contribuye a la formación de la opinión pública libre. Como bien ejemplifica Steiger, mientras que la publicidad política televisada es «visible para todos y abierta al control público», la forma en la que funcionan los algoritmos de las redes sociales no es transparente y carece de «un espacio público de resonancia en el que los anuncios puedan discutirse y cuestionarse»[30].

---

[25] *Ibid.* p. 350.

[26] *Ibid.* p. 351.

[27] «Píxel de Meta», Meta, acceso el 16 de diciembre de 2022, *https://es-es.facebook.com/business/tools/meta-pixel*.

[28] Puede incrementar la polarización del electorado, pues posibilita identificar grupos que son más susceptibles de ser influenciados. Blasi Casagra y Vermueulen, «Reflections on the murky legal practices», 349.

[29] Como ha señalado el Comité Europeo de Protección de Datos, «la extensión de estas técnicas de tratamiento de datos a fines políticos plantea graves riesgos, no solo a los derechos a la privacidad y a la protección de datos, sino también a la confianza en la integridad del proceso democrático», y afecta a otros derechos fundamentales «como la libertad de expresión y la libertad de opinión y la posibilidad de pensar libremente sin manipulación». Comité Europeo De Protección De Datos, *Declaración 2/2019 sobre el uso de datos personales durante las campañas políticas* (13 de marzo de 2019): 1.

[30] No existen las opiniones diversas y el pluralismo se pone en peligro. Steiger, «International law», 82-83.

2. BURBUJAS DE FILTRO: COMO SE ESTÁ RESTRINGIENDO LA INFORMACIÓN QUE CONSULTAMOS A TRAVÉS DE LAS REDES

Hoy en día las redes sociales se han convertido en la principal fuente de información para muchos usuarios. La gente más joven principalmente se informa a través de X, Facebook, Twitter, Instagram[31]. El problema es que la información que nos llega a través de estas plataformas está personalizada. Cuando buscamos información en Google, compartimos noticias en Facebook, o miramos un video en YouTube, estamos proporcionando una información que los algoritmos de estas plataformas utilizan para ofrecerte publicidad o contenidos similares. Estos sistemas de recomendación funcionan utilizando lo que se denominan «filtros colaborativos», es decir, no solo utilizan tus datos sino también los de otros usuarios para predecir tus preferencias, y solo recomendarán los contenidos que superen el filtro[32].

La forma en que funcionan estos sistemas de recomendaciones y filtros colaborativos puede verse con el siguiente ejemplo[33]: tenemos la información del historial de compra de seis clientes de un supermercado online y fijamos como hipótesis que después de comprar artículos similares probablemente otros usuarios comprarán un mismo artículo:

USUARIO	HISTORIAL DE COMPRA				COMPRA MÁS RECIENTE
A	Fresas	Pollo	Galletas	Pan	Café
B	Kiwis	Café	Leche	Café	Café
C	Leche	Paté	Peras	Carne	Agua
D	Agua	Leche	Pavo	Yogures	Pan
E	Fresas	Café	Leche	Café	¿?

Fuente: Elements of AI

La tarea sería predecir cuál podría ser la compra más reciente del cliente E. Para ello habría que calcular la similitud del cliente E con el resto de los clientes, que son los datos que se han recopilado y que el algoritmo tendría como datos de entrenamiento (sumando el número de compras similares de

[31] Ha aumentado la desconfianza en este nivel de población hacia los medios tradicionales, y la mayoría afirma que se informa a través de las redes sociales. Sergio Giraldo Luque y Cristina Fernández Rovira, «¿Radicalizan a los jóvenes las redes sociales?», *The Conversation*, 4 de marzo de 2025, acceso el 5 de marzo de 2025 *https://theconversation.com/topics/jovenes-59211*.

[32] Curso Elements of IA, Capítulo 4. II, University of Helsinky. Curso online gratuito disponible en *www.elementsofai.com*

[33] Ejemplo adaptado del proporcionado en el curso Elements of IA de la Universidad de Helsinki. *Ibid.*

cada cliente). Una vez calculadas las similitudes, se identificaría al usuario más similar a E, seleccionando la mayor de las similitudes calculadas que sería con el cliente B.

USUARIO	SIMILITUD CLIENTE E CON RESTO CLIENTES
A	1
B	3
C	1
D	1

Fuente: Elements of AI

Luego, atendiendo a que la compra más reciente del cliente B fue café, el algoritmo predeciría y, por tanto, sugeriría al cliente E como siguiente compra también café.

Evidentemente, cuantos más datos más «fiable» será la predicción. Pero nos sirve como ejemplo para ilustrar cómo funcionan los sistemas de recomendación de noticias y contenido en redes sociales.

Por lo tanto, los contenidos que no «te gusten» (o, mejor dicho, que el algoritmo predice que no te gustarán) no superarán el filtro y no se mostrarán. Esto puede conducir a lo que se ha denominado *burbujas de filtro*[34]. Todo se adapta a los intereses del usuario, la información también. Dejamos por tanto de ver las opiniones diversas o contrapuestas a las nuestras. Si bien hay estudios que argumentan que la existencia de estas burbujas de filtro es limitada y que hay poca evidencia que demuestre que los usuarios de redes sociales están más polarizados que los no usuarios[35], si uno observa la publicidad e información que aparece cuando utiliza, por ejemplo, YouTube puede darse cuenta perfectamente que los resultados que se muestran coinciden con sus preferencias personales. Cuando se consulta una determinada noticia, automáticamente el algoritmo empieza a recomendar noticias similares. Es cierto que esto también es consecuencia de la actual sociedad más individualizada en la que vivimos, en la que los individuos tienden a reafirmarse en sus convicciones pese a que se les muestren datos que confrontan estas. Por otra parte, si pueden encontrarse estudios que muestran que a mayor cantidad de información se produce mayor polarización, pues los usuarios tienden a

[34] Término introducido por Eli Praiser en su libro de 2017, en el que señala como la burbuja de filtros sesga nuestra percepción del mundo. Eli Praiser, *El filtro burbuja. Cómo la red decide lo que leemos y lo que pensamos* (Taurus, 2017): introducción. Previamente, Sunstein había introducido el término «Cámaras de eco» en su libro Cass Sustein, *Republic.com* (Princeton University Press, 2001).

[35] Señalando que realmente los algoritmos no restringen la diversidad de información a la que estamos expuestos. Puede verse, a este respecto, el artículo de Axel Bruns, «El Filtro Burbuja», *Revista Latinoamericana de Economía y Sociedad Digital*, n.º especial 1 (julio, 2022), doi.org/10.53857/ndhq9707.

compartir las noticias que concuerdan con su ideología y a alejarse de noticias y grupos que no comparten su visión[36].

El problema, a nuestro entender, se plantea cuando esta forma de funcionamiento de los algoritmos se combina con las técnicas de *microtargeting* empleadas durante las campañas electorales, y se transmite de esta forma información falsa o sesgada para tratar de generar polarización e influir en la intención de voto. Ya en la campaña que llevó a la Presidencia a Donald Trump Cambridge Analytica utilizó una metodología del campo militar que adaptó a las redes sociales, elaborando campañas personalizadas que generaban información distinta para cada usuario de acuerdo con sus ideales y convicciones[37], técnica que ha vuelto a emplear en 2024 con el apoyo de X de Elon Musk[38], en la que se ha podido identificar cómo se ha enviado propaganda personalizada a votantes musulmanes y judíos definiendo a Kamala Harris como «proisraelí» o «propalestina» respectivamente[39].

Como se ha puesto de relieve con el ejemplo empleado, los algoritmos priorizan el contenido que entienden va a gustar al usuario, lo que las técnicas de *microtargeting* aprovechan para segmentar las audiencias y enviar propaganda personalizada que refuerza los gustos expresados por este. No es solo que se reciban mensajes segmentados, sino que los algoritmos amplifican los que van a generar más reacciones por parte del usuario[40]. Y este

---

[36] Puede verse a este respecto el estudio de Andrejevic y Volcic, en el que partiendo de los trabajos de Pairser y Sunstein, entre otros autores, reexaminan el concepto del filtro burbuja, y en el que si bien también destacan como hay autores que contestan la evidencia de la existencia de estos filtros burbuja, si hay estudios que demuestran esa existencia de mayor polarización en la actualidad. Mark Andrejevic y Zola Volcic, «From mass to automated media. Revisiting the "filter bubble"» en Big *Data, Political Campaigning and the Law. Democracy and Privacy in the age of microtargeting*, edited by Normann Witzledb, Moira Paterson and Janice Richardson, (New York: Routledge, 2020),18-22.

[37] Carlos Merlo, *Data Science Electoral* (México: Anderson Publishing, 2021), 75.

[38] Sebastián Silva C., «Donald Trump y Elon Musk: la desinformación al poder», *Sinc*, 5 de febrero de 2025, acceso el 7 de febrero de 2025, *https://www.agenciasinc.es/Opinion/Donald-Trump-y-Elon-Musk-la-desinformacion-al-poder*; Anwar Ashraf, «Las mentiras de Elon Musk sobre las elecciones en EE.UU.», *DW*, 2 de noviembre de 2024, acceso el 7 de febrero de 2025, *https://www.dw.com/es/dw-verifica-c%C3%B3mo-elon-musk-est%C3%A1-difundiendo-mentiras-sobre-las-elecciones-estadounidenses/a-70685868*. Los anuncios contra Kamala Harris han sido pagados por Future Coalition PAC, organización que solo había recibido una donación de 3 millones de dólares de Building America's Future, a la que en 2022 Musk donó 50 millones de dólares. «"Kamala Harris proisraelí" si eres musulmán y "propalestina" si eres judío: así acaban donaciones de Elon Musk en anuncios contra la candidata demócrata», Maldita.es, 21 de octubre de 2024, acceso el 7 de febrero de 2025, *https://maldita.es/malditatecnologia/20241021/anuncios-musk-contra-kamala-harris/*

[39] La localización geográfica ha sido también un factor utilizado, apuntando a los Estados donde mayor población hay de esos colectivos (Michigan - votantes árabe-musulmanes, o Pensilvania-votantes judíos). *Ibid.*

[40] Un análisis de cómo los algoritmos privilegian el potencial de viralización de un contenido o noticia, puede consultarse en Jeff Horwitz, *Broken Code. Inside Face-*

tipo de noticias falsas se difunden mucho más rápido y de forma más amplia que las verdaderas, como concluye un estudio realizado por investigadores del MIT en 2018[41]. Difusión en la que el factor humano contribuye más que el uso de *bots*, pues ya no es que esas personas estén expuestas a información diversa que quieran criticar, sino que directamente están recibiendo información falsa o sesgada que reproducen en sus redes sociales, contribuyendo a incrementar esa polarización. Por ello, el estudio mencionado recomienda que las políticas de contención de la desinformación deberían también hacer hincapié en las intervenciones conductuales, como el etiquetado y los incentivos para disuadir de la difusión de desinformación[42]. Pero, en último término, también es responsabilidad de cada persona mantenerse informada y contrastar distintos medios, dudar de las noticias muy sensacionalistas o que se ven claramente polarizadas y no conformarse con una sola fuente de información. Compartimos, por tanto, con Andrejevic y Volcic que actualmente falta un espacio en el que se puedan tener en cuenta las opiniones de los demás y crear un interés público compartido[43]. Y esto puede lograrse educando desde una edad temprana en una mayor solidaridad y respeto a las opiniones diversas, y en una concienciación en la necesidad de contrastar información[44].

---

book and the fight to expose its harmful secrets (New York: Doubleway, 2023). Así, por ejemplo, Horwitz cita en el libro el análisis realizado por Carig Silerman, reportero de BuzzFeed, que mostraba que en los meses finales de las elecciones estadounidenses de 2016 las noticias falsas habían sido el contenido más viralizado en Facebook. Jeff Horwitz, *Broken Code…,* 1980.

[41] El estudio investigó la difusión diferencial de todas las noticias verificadas, verdaderas y falsas, distribuidas en Twitter entre 2006 y 2017, en el que se destaca como las noticias falsas tienen un 70 por 100 más de probabilidades de ser retuiteadas. Soroush Vosoughi, Deb Roy, Sinan Aral, «The Spread of true and false news online», *Science* 359, issue 6380 (2018): 1 y 4, DOI: 10.1126/science.aap9559.

[42] *Ibid.* p. 5. Piore, en un artículo de la MIT Technolgy review, cita las propuestas realizadas por diversos especialistas, señalando entre ellos a Zuckerman, que propone la creación de una plataforma pública de redes sociales con una misión cívica, que pudiese volcar opiniones desconocidas en nuestros canales y sacarnos de nuestra zona de confort. Adam Piore, «Technologists are trying to fix the "filter bubble" problem that tech helped create», *MIT Technology Review* (22/8/2018), acceso el 20 de febrero de 2025, *https://www.technologyreview.com/2018/08/22/2167/technologists-are-trying-to-fix-the-filter-bubble-problem-that-tech-helped-create/*.

[43] Andrejevic y Volcic, «From mass to automated media», 17-18 y 32-33. Sunstein señala que para una democracia saludable son necesarios espacios públicos compartidos, que son mejores que las «cámaras de eco». Sunstein, *Republic.com*, 205.

[44] Porque, para ser más precisos, actualmente hemos evolucionado hacia democracias más débiles, se ha producido un cambio en nuestra forma de relacionarnos hacia un mayor individualismo, lo que ha sabido aprovechar el neoliberalismo y los grandes mercados. Un estudio interesante que conecta este cambio en nuestras democracias y la evolución de nuestro comportamiento con la idea de los filtros burbuja en Janice Richardson, «Filter bubbles, democracy and conceptions of self. A brief genealogy and a Spinozist perspective» en Big *Data, Political Campaigning and the Law. Democracy and Privacy in the age of micro-targeting*, edited by Normann Witzledb, Moira Paterson and Janice Richardson, (New York: Routledge, 2020), 34-46.

En resumen, la combinación de los algoritmos de las plataformas y redes y las técnicas de *microtargeting* crea un entorno en el que la información fluye de forma asimétrica, en el que se ve reforzada la difusión de desinformación y se genera mayor polarización. Es por ello por lo que es necesario abordar este problema adoptando normativa que permita proteger mejor los datos de los usuarios e impedir un uso indebido de este tipo de técnicas, lo que trataremos de exponer en el apartado dedicado a la normativa europea en vigor.

3. LOS EFECTOS DEL USO DE TÉCNICAS DE *MICROTARGETING* PARA LA DIFUSIÓN DE DESINFORMACIÓN EN PROCESOS ELECTORALES Y EN LOS DERECHOS FUNDAMENTALES

Como se ha adelantado en la introducción del presente trabajo, la proliferación de información falsa y de tácticas de desinformación se ha extendido y se ha vuelto más sofisticada técnicamente en los últimos años. La publicidad es, en este sentido, uno de los vehículos más importantes para la difusión de desinformación. Como señala Leticia Rodríguez, en Internet los anunciantes pagan por audiencias en lugar de espacios (publicidad programática), pues lo importante es llegar al mayor número de personas posible, independientemente del espacio en el que se inserte la publicidad. El contenido no importa, solo el tráfico que se genera, por lo que nos encontramos con que muchos medios de desinformación aprovechan noticias falsas, partidistas o xenófobas para generar *clicks* rápidos y obtener ganancias con los anuncios publicitarios asociados a sus páginas[45].

Ya en un informe de 2019 la Comisión de Venecia aborda el impacto de las redes sociales y de Internet en los procesos electorales, destacando como las técnicas de manipulación del comportamiento pueden amenazar la autenticidad del sufragio, la equidad de los procesos electorales y, en último término, la capacidad de traducir el deseo del pueblo en representación institucional y decisiones de gobierno[46]. Aunque estas amenazas ya existían, señala la Comisión, las posibilidades que ofrecen las nuevas tecnologías han incrementado los riesgos y limitan las posibilidades de las instituciones y autoridades para mantener un equilibrio en las reglas de juego de la comunicación electoral[47].

Cuando se hace un uso indebido de las técnicas de *microtargeting* y se difunde información falsa para tratar de manipular el comportamiento de los electores, los principios que deben garantizar toda competición electoral (objetividad, neutralidad política, transparencia e igualdad de armas), como des-

---

[45] Leticia Rodríguez Fernández, *Propaganda digital. Comunicación en tiempos de desinformación*. (Barcelona: Editorial UOC, 2021), 104.

[46] *Joint Report of the Venice Commission on Digital Technologies and Elections*, apdo. 36.

[47] *Ibid*, apdos. 36 a 38.

taca Rosario García Mahamut, pueden verse afectados[48], así como toda una serie de derechos fundamentales y valores consagrados constitucionalmente.

En primer lugar, se puede ver afectada la formación de una opinión pública libre que, como ha señalado el Tribunal Constitucional, viene garantizada por las libertades del artículo 20 de la Constitución. Dicho artículo, en sus distintos apartados, garantiza el mantenimiento de una comunicación pública libre sin la cual, señala el Tribunal, otros derechos que la Constitución consagra quedarían vaciados de contenido real y absolutamente falseado el principio de legitimidad democrática, base de nuestra ordenación jurídico-política[49]. Porque, como continúa su argumentación nuestro Alto Tribunal, para que el ciudadano pueda formar libremente sus opiniones y, de esta forma, participar de modo responsable en los asuntos públicos, ha de ser informado de forma que pueda contrastar/ponderar opiniones diversas y contrapuestas[50].

Formación de una opinión pública libre que, recuerda el Tribunal, está «indisolublemente ligada con el pluralismo político»[51], que también se ve afectado, pues la combinación de dichas técnicas con la forma en la que funcionan las redes sociales y sistemas de recomendación —que crean las denominadas burbujas de filtro tal y como se ha examinado en el apartado 3— tienen como efecto que al elector no solo se le muestra información falsa o sesgada, sino que no le llegan esas informaciones u opiniones diversas y contrapuestas, por lo que no podrá realizar esa ponderación o contraste al que hace referencia el Tribunal constitucional. Por lo tanto, si los partidos políticos pueden recopilar las opiniones políticas de los ciudadanos y se posibilitan técnicas como las empleadas en la campaña electoral de EE. UU. de 2016, la formación de esta opinión pública libre y de ese pluralismo político puede quedar afectada[52].

Además, puede decirse que el derecho a participar en los asuntos públicos por medio de representantes libremente elegidos, consagrado por el art. 23.1 CE, también se vería afectado pues, como ha señalado el TC, se trata de un derecho que encarna el derecho de participación política en el sistema democrático de un Estado social y democrático de Derecho[53], por lo que el uso de técnicas de *microtargeting* puede afectar a la libertad con la que los

---

[48] García Mahamut, «Partidos políticos y derecho a la protección de datos», 309-310.

[49] STC 90/1990, FJ 4, con cita a la STC 6/1981.

[50] *Ibid.*, con cita a la STC 159/1986, FJ 6.

[51] *Ibid.*

[52] Rosa María García Sanz, «Tratamiento de datos personales de las opiniones políticas en el marco electoral: todo en interés público», *Revista de Estudios Políticos*, 183 (2019), 137, doi: *https://doi.org/10.18042/cepc/rep.183.05*; Andoni Polo Roca, «Protección de datos y elaboración de perfiles: el nuevo artículo 58 bis de la Ley orgánica 5/1985, de 19 de junio, del régimen electoral general», *Revista Galega de Administración Pública (REGAP)* núm. 58 (julio-diciembre 2019), 522-523, doi: 10.36402/regap.v1i58.46.

[53] STC 119/1995, de 17 de julio, FJ 2.

ciudadanos pueden realizar la elección de sus representantes. El artículo 25 del Pacto Internacional de los Derechos Civiles y Políticos, y el artículo 3 del Protocolo Adicional del CEDH también garantizan este derecho de los ciudadanos a participar en los asuntos públicos por medio de la elección de sus representantes. Elecciones que, como señala la Oficina del Alto Comisionado para los Derechos Humanos «deben celebrarse con una periodicidad que garantice que la autoridad del Gobierno sigue basándose en la libre expresión de la voluntad de los electores»[54], en las que las personas puedan elegir libremente a los candidatos y votar a favor de cualquier propuesta «sin influencias indebidas ni coacción de ningún tipo que pueda distorsionar o inhibir la libre expresión de la voluntad del elector»[55]. Los votantes, añade, deben poder formarse una opinión de forma independiente sin que se de ningún tipo de interferencia o manipulación[56]. Esto muestra, como señala Steiger, que los Estados deben proteger sus elecciones tanto frente a injerencias internas como externas[57], que a través de la desinformación tratan de influir en los resultados electorales.

Por otra parte, tal y como se ha adelantado en el apartado 2 se pueden utilizar una gran variedad de datos como edad, sexo, lugar de residencia, etc. para segmentar las audiencias y dirigir una determinada publicidad o propaganda electoral. Y, aunque de esos datos directamente no se infiera la ideología política de una determinada persona, indirectamente de su combinación y de las noticias e información que los usuarios comparten sobre temas de su interés, sí puede obtenerse dicha información. Es, por este motivo, que la recopilación de datos relativos a las opiniones políticas de las personas para realizar técnicas de *microtargeting* electoral debe estar absolutamente prohibida pues, además de que se estaría vulnerando el derecho a la protección de datos, puede entenderse que se estaría vulnerando también el derecho a la libertad ideológica. De acuerdo con el artículo 16.2 CE nadie podrá ser obligado a declarar sobre su ideología. Pero, además, en el apartado 1 de dicho artículo se consagra la libertad ideológica que, como ha destacado el Tribunal Constitucional, es una libertad esencial para la efectividad de los valores superiores de nuestro ordenamiento jurídico y, en especial, para el pluralismo político al que se ha hecho referencia anteriormente[58].

En resumen, las nuevas tecnologías pueden utilizarse para facilitar la formación de la opinión pública, permitiendo una mayor participación y fo-

---

[54] CCPR, General Comment No. 25: Article 25 (Participation in Public Affairs and the Right to Vote), The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service, ap. 9.

[55] *Ibid.* ap. 19.

[56] *Ibid.*

[57] Steiger, «International law», 88. En palabras del TEDH, los Estados tienen, en virtud del art. 3 del protocolo adicional del Convenio, una obligación de adoptar medidas positivas para celebrar elecciones democráticas. TEDH (Pleno), *Mathieu-mohin and Clerfayt vs. Belgium*, 2 marzo 1987, ap. 50.

[58] STC 20/1990, de 15 de febrero, FJ 3.

mentando el pluralismo político. Pero también permiten influir en el comportamiento del elector y difundir información falsa, lo que puede afectar no solo a los principios que rigen la campaña electoral (libre concurrencia, competitividad e igualdad de oportunidades), sino también a la formación de la opinión pública a la que los partidos políticos han de concurrir[59]. Es necesario, por tanto, comenzar a actuar para hacer frente a estas nuevas técnicas de manipulación, pero otra cuestión distinta es que para luchar contra las mismas se deba permitir la creación de bases de datos con perfiles ideológicos por parte de los partidos políticos, tal y como trató de hacer el artículo 58bis de la LOREG declarado inconstitucional por el TC[60]. Porque, como señala Rosa María García Sanz, la limitación del derecho a la protección de datos permitiendo que los partidos políticos recopilen las opiniones políticas de los ciudadanos podría llevar a la paradoja de terminar desnaturalizando el derecho de sufragio[61]. Por el contrario, la democracia sí podría servir como base para limitar aquellas interferencias en los derechos fundamentales que sean desproporcionadas, como propone Steiger, y luchar así contra prácticas como las llevadas a cabo por Cambridge Analytica o Project Lakhta, de forma que se proteja el derecho a la participación democrática y a la privacidad[62].

---

[59] Arenas Ramiro, «Partidos políticos», 350-351.

[60] STC 76/2019, de 22 de mayo. La AEPD, ya incluso antes de la votación de la Ley, trató de clarificar la modificación señalando que no permitía la recopilación de esos datos para elaborar perfiles ideológicos ni el envío de propaganda personalizada basada en los mismos, sino que sólo permitía a los partidos recopilar información para «pulsar las inquietudes de los ciudadanos» y así poder darles respuesta en sus propuestas electorales. AEPD, *Criterio de la Agencia Española de Protección de Datos sobre cuestiones electorales en el proyecto de nueva LOPD*, 21 de noviembre de 2018, acceso el 20 de enero de 2024, www.aepd.es. No obstante, los principales expertos en la materia ya destacaban antes de la aprobación que el nuevo apartado 1 del artículo 58 bis no se ajustaba a lo previsto en el RGPD y sí posibilitaba la creación de bases de datos con las opiniones políticas de los ciudadanos. Rosario G. Gómez, «La nueva ley de protección de datos alarma a los expertos», *El País*, 3 de diciembre de 2018 (que recoge las opiniones de Borja Adsuara, Tomás de la Quadra-Salcedo y Carlos Sánchez Almeida), acceso el 10 de febrero de 2025, *https://elpais.com/sociedad/2018/12/02/actualidad/1543765290_001106.html.* Andoni Polo Roca, «Protección de datos», 520.

[61] Derecho de sufragio que ya no sería libre y secreto, pues mediante los medios tecnológicos los partidos políticos podrían elaborar bases de datos de las opiniones políticas de los electores que les permitirían en cierto modo determinar el voto del elector. Lo que no serviría, señala la autora, para la formación de la opinión pública libre que el funcionamiento democrático requiere. Rosa María García Sanz, «Tratamiento de datos personales», 135. Sobre el uso de las nuevas tecnologías en los procesos electorales y las amenazas que supone, puede consultarse también el trabajo de Rafael Rubio Núñez, «La amenaza tecnológica en los procesos electorales: una respuesta jurídica», *Revista de privacidad y derecho digital*, vol. 3, Núm. 11, (julio-septiembre 2018): 109-146.

[62] Steiger, «International law», 93. Ambos casos son explicados por el autor citado. Al asunto Cambridge Analityca ya hemos hecho referencia más detenidamente anteriormente en este trabajo. En cuanto a Project Lakhta, se trató de una operación de desinformación llevada a cabo por la Agencia de Investigación de Internet rusa

4. NORMATIVA EUROPEA APLICABLE A LAS TÉCNICAS DE *MICROTARGETING* ELECTORAL

Como se ha adelantado en los apartados precedentes, la utilización incorrecta de técnicas de *microtargeting* electoral para difundir desinformación está poniendo en peligro la integridad de los procesos electorales, facilitando la proliferación de campañas de desinformación que buscan polarizar e influir en los resultados de dichos procesos. Se trata de unas prácticas que desbordan las posibilidades de acción individual de los Estados miembros por lo que, como muy acertadamente examina Miryam Rodríguez Izquierdo, una serie de normativas adoptadas a nivel de la Unión pueden servir para ir estableciendo una serie de garantías para los procesos electorales y luchar contra la desinformación[63].

En primer lugar, el Reglamento General de Protección de datos, pues las normas que establece para el tratamiento lícito de los datos personales han de ser respetadas por las plataformas digitales que son de las que principalmente se obtienen los datos necesarios para realizar las prácticas de *microtargeting* electoral. En segundo lugar, el Reglamento sobre transparencia y segmentación de la publicidad política, que buscar contrarrestar la manipulación de la información y la injerencia extranjera en las elecciones[64]. Y, en tercer lugar, otras normas de la Unión que pueden ser de aplicación a las prácticas examinadas, como los Reglamentos de Servicios y Mercados Digitales, y el Reglamento de IA, que buscan mejorar el funcionamiento del mercado interior estableciendo un marco jurídico uniforme en tres ámbitos en los que las empresas y operadores implicados pueden coadyuvar en la lucha contras las prácticas de *microtargeting* electoral y contra la desinformación[65].

---

para influir en la opinión pública y en las elecciones en EE.UU (mediante el robo de datos personales de ciudadanos estadounidenses, para publicar comentarios ofensivos y que generasen división entre los votantes), para disuadir el voto hacia Hillary Clinton y aumentar el apoyo a Trump. *Ibid.* pp. 75 y 76.

[63] Señala la autora que, cuando la Unión Europea actúa para regular el mercado interior y establece las normas que las plataformas digitales deben respetar, se consigue de forma colateral la protección de la información de interés público y del electoral. Miryam Rodríguez-Izquierdo, «El mercado interior y la manipulación informativa con finalidad electoral» (Comunicación presentada al XXI Congreso de la ACOES: Constitución y Elecciones, Valladolid, 27 y 28 de marzo de 2024), 6.

[64] «La UE introduce nuevas normas sobre transparencia y segmentación en la publicidad política», Consejo De La Unión Europea, 11/3/2024, acceso el 10 de marzo de 2025, *https://www.consilium.europa.eu/es/press/press-releases/2024/03/11/eu-introduces-new-rules-on-transparency-and-targeting-of-political-advertising/*.

[65] Conviene destacar también en materia de IA el Convenio Marco sobre IA adoptado por el Consejo de Europa que, como señala Mario Hernández Ramos, es complementario al Reglamento Europeo, y se ha centrado en el desarrollo y aplicación de los sistemas de IA «desde el punto de vista de su impacto en los derechos humanos, la democracia y el Estado de Derecho». Mario Hernández Ramos, «La Convención Marcos

Todas estas normas son de aplicación uniforme en todos los Estados miembros, si bien en algunos aspectos dejan margen de actuación a nivel interno. Pero, como se examinará a continuación, pueden servir para luchar a nivel de toda la UE contra el uso indebido de las prácticas de *microtargeting* electoral y la difusión de desinformación a través de estas.

Hay que señalar que, evidentemente, aparte de la normativa adoptada a nivel de la UE la jurisprudencia del Tribunal de Justicia de la Unión Europea juega un papel también muy importante por lo que respecta a la protección de datos personales, privacidad y responsabilidad de las plataformas digitales[66]. Por el objeto y extensión del presente trabajo no procede realizar un análisis pormenorizado de esta jurisprudencia, pero sí puede apuntarse que, aunque la misma no trate de forma directa sobre la difusión de desinformación, si puede entenderse que indirectamente coadyuva a que se limiten las posibilidades de su difusión. Así, por ejemplo, en el asunto *Glawischnig-Piesczek vs. Facebook* el TJUE estableció que los prestadores de servicios de alojamiento de datos pueden ser obligados a eliminar contenido difamatorio declarado ilícito, o a bloquear el acceso al mismo, a nivel mundial, y sin que ello vulnere la libertad de expresión. Se trata de garantizar la protección de la persona víctima de actos difamatorios, en los casos en que la plataforma tiene conocimiento de la información ilícita y un tribunal está solicitando dicha eliminación[67]. De esta forma, se logra que no se mantengan noticias o contenidos declarados ilícitos en plataformas o redes sociales, contribuyendo al mantenimiento de la difusión de desinformación.

4.1. El RGPD

Como se ha examinado en los apartados precedentes, a través de los datos que compartimos a través de las redes sociales es posible inferir los datos relativos a las opiniones políticas de una persona, para así tratar de influir en su intención de voto. Por lo tanto, como señala McDonagh, es necesario considerar la legitimidad del tratamiento de todas las categorías de datos personales con fines electorales[68]. Así, partiendo del artículo 6.1 del Reglamento

---

del Consejo de Europa sobre inteligencia artificial y derechos humanos, democracia y Estado de Derecho. El primer tratado internacional en la materia», en *Fortalecimiento de la democracia y el Estado de Derecho a través de la inteligencia artificial*, ed. por Rafael Bustos Gisbert, Javier García Roca (Oñati: IVAP, 2025): 119

[66] Así, algunas sentencias clave en materia de protección de datos que pueden citarse del TJUE son *Google España c. AEPD y Mario Costeja González*, asunto C-131/12, sobre derecho al olvido; *Schrems* I, asunto C-362/14, y *Schrems* II, asunto C-311/18, sobre la anulación del Escudo de Privacidad por la insuficiente protección de datos en los EE.UU.; o *La Quadrature du Net vs. France*, asuntos acumulados C-511/18, C-512/18 y C-520/18, sobre los límites a la vigilancia masiva de datos en la UE.

[67] Sentencia del Tribunal de Justicia (Sala Tercera) de 3 de octubre de 2019, *Eva Glawischnig-Piesczek contra Facebook Ireland Limited*, asunto C-18/18, apdos. 21 a 53.

[68] Maeve McDonagh, «Freedom of processing of personal data for the purpose of electoral activities after the DGPR» en *Big Data, Political Campaigning and the Law.*

General de Protección de Datos (en adelante, RGPD), para que el tratamiento sea lícito debe cumplirse, al menos, una de las condiciones establecidas en dicho artículo que parte, como no podría ser de otra forma, del consentimiento del interesado para el tratamiento de sus datos personales para uno o varios fines específicos[69]. El tratamiento de datos durante campañas electorales debe respetar lo dispuesto en este artículo y, en particular, en sus letras e) —tratamiento necesario para una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento— y f) — tratamiento necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño—[70].

Por lo que al presente estudio interesa, el RGPD contiene también disposiciones específicas respecto a los datos relativos a las opiniones políticas de las personas, los cuales considera datos especialmente protegidos (artículo 9.1 RGPD)[71], quedando su tratamiento prohibido salvo que concurra alguna de las circunstancias que el propio Reglamento contempla, en concreto:

— Que el interesado haya dado consentimiento explícito para el tratamiento de dichos datos con uno o más de los fines especificados (art. 9.2.a) RGPD).

— Que el interesado los haya hecho manifiestamente públicos (art. 9.2.e) RGPD).

— Que su tratamiento sea necesario por razones de un interés público esencial, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer las medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado (art. 9.2.g) RGPD).

Ahora bien, debe tenerse en cuenta dos aspectos: por un lado, debe examinarse si el artículo 9 por sí mismo establece condiciones suficientes y más

---

Democracy and Privacy in the age of micro-targeting. Edited by Normann Witzledb, Moira Paterson and Janice Richardson (New York: Routledge, 2020), 117.

[69] Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *DOUE* nº 119, de 4 de mayo de 2016 (en adelante, RGPD).

[70] Para más información al respecto, McDonagh, «Freedom of processing of personal data», 120-124.

[71] Además de estos datos, el citado artículo considera categoría de datos especiales otra serie de datos especialmente sensibles como son los que revelen el origen étnico o racial, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o a la orientación sexual de una persona física.

estrictas, o si exige una aplicación acumulativa con el artículo 6 para garantizar una completa protección de los interesados, tal y como ha señalado el grupo de trabajo del artículo 29[72]; por otro, que el RGPD hace un reenvío al Derecho de la Unión o al de los Estados miembros a efectos de que desarrollen estas circunstancias[73] y, de esta forma, especifiquen si por ejemplo la prohibición del tratamiento de dichos datos no puede ser levantada por el consentimiento explícito del interesado, o si el tratamiento puede realizarse por razones de un interés público esencial. Así, por ejemplo, el legislador español ha establecido que no basta el solo consentimiento del afectado para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología (art. 9.1 LOPDGDD), y que el tratamiento por razones de un interés público esencial debe estar amparado en una norma con rango de ley que podrá establecer requisitos adicionales relativos a la seguridad y confidencialidad de estos datos (art. 9.2 LOPDGDD)[74].

Por lo tanto, en cuanto a la elaboración de perfiles ideológicos[75], las prácticas de *microtargeting* electoral deben respetar también estas disposiciones del RGPD. Es decir, el tratamiento de datos personales relativos a las opiniones políticas de las personas solo será posible cuando se respete lo establecido en el artículo 9.2 del RGPD. Y con respecto al tratamiento por parte de los partidos políticos debe atenderse a lo establecido en el considerando 56 del RGPD que señala que «si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas». Es decir, conforme a este considerando, se podrá autorizar el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan las garantías adecuadas, y en los casos en que

---

[72] Por lo tanto, si un responsable está tratando categorías especiales de datos no puede invocar solo el artículo 6 para legitimar el tratamiento, sino que debe aplicarlo junto con el artículo 9 para garantizar que se cumplen todas las garantías y medidas pertinentes. «Dictamen 6/2014», Grupo de Trabajo sobre Protección de Datos del artículo 29 de 9 de abril de 2014 (hay que aclarar que el dictamen hace referencia a los artículos de la anterior directiva, pero que sigue siendo de aplicación a lo actualmente previsto por el RGPD), 17-19.

[73] En su considerando 10, el RGPD reconoce un margen de maniobra a los Estados miembros para que desarrollen sus normas, incluidas las circunstancias en las que se pueden tratar las categorías especiales de datos personales.

[74] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *BOE* nº 294, de 6 de junio de 2018 (en adelante, LOPDGDD).

[75] De acuerdo con el Reglamento, se entiende por elaboración de perfiles «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física» (art. 4.4) RGPD)

el funcionamiento del sistema democrático exija posibilitar ese tratamiento, lo que se dará sólo en ciertas circunstancias, siempre como señala Hernández Peña que ello sea establecido en una norma jurídica, de forma restringida y sujeto a unas garantías[76]. Interés público que, además, debe ser esencial, tal y como señala el TC en su sentencia 76/2019 en la que declaraba inconstitucional el artículo 58bis de la LOREG al no identificar, entre otras cuestiones, el interés público esencial que fundamentaría la restricción del derecho fundamental a la protección de datos[77]. Por lo tanto, no es solo un interés público, sino que debe ser un interés que sea fundamental para el funcionamiento del Estado democrático, tal y como exige el mencionado considerando 56.

Por lo tanto, solo en los supuestos señalados los partidos políticos podrían realizar un tratamiento de estos datos. Fuera de estos supuestos, los partidos sólo pueden gestionar los datos de sus afiliados[78], como prevé la letra d) del apartado 2 del artículo 9 del RGPD[79].

Ahora bien, la redacción dada a este considerando ha sido ampliamente criticada, pues utiliza términos poco precisos y excesivamente amplios como «actividades electorales», «si el funcionamiento democrático lo exige» o «razones de interés público esencial»[80]. Tal y como viene reiterando la jurispru-

---

[76] Juan Carlos Hernández Peña, «Campañas electorales, Big Data y perfilado ideológico. Aproximación a su problemática desde el derecho fundamental a la protección de datos», *Revista Española de Derecho Constitucional*, 124 (2022): 54, doi: *http$3doi.org/10.18042/cepc/redc.124.02*.

[77] STC 76/2019, de 22 de mayo, FJ 7. Es decir, no bastaría un mero interés público, sino que este deberá ser esencial, si bien el TC en la sentencia citada no define que debe entenderse por este, como tampoco define claramente en otras sentencias el concepto de interés público, tal y como señala López Calera, que destaca como la indeterminación del concepto termina trasladada también a la jurisprudencia, por lo que el interés público termina siendo decidido con un argumento de autoridad, pero no es objetivable. Por ello, propone como concepto más razonable de interés público aquel que «vincula su constitución y su aplicación a principios democráticos». Nicolás López Calera, «El interés público: entre la ideología y el Derecho», *Anales de la Cátedra Francisco Suárez* nº 44 (2010): 146 y ss, doi: *https://doi.org/10.30827/acfs.v44i0.502*.

[78] Arenas Ramiro, «Partidos políticos», 347-349.

[79] El tratamiento por parte de «asociaciones, fundaciones u otros organismos sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical», caso en el que entrarían los partidos políticos, solo se permite cuando es efectuado «en el ámbito de sus actividades legítimas» y con las debidas garantías, referido exclusivamente a los «miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados» (art. 9.2.d RGPD). De nuevo, el principal problema es la amplitud de la excepción y que tampoco se define que son las «debidas garantías» o las «actividades legítimas». McDonagh, «Freedom of processing of personal data», 126-127.

[80] Lo que, como señala Rosa García Sanz, resulta llamativo cuando se está ante un asunto de gran importancia donde confluyen el derecho a la protección de datos, el de participación política, el derecho de sufragio, el derecho a la libertad ideológica y el derecho a la libertad de expresión e información. García Sanz, «Tratamiento de datos personales», 132-133.

dencia del Tribunal Constitucional, del TJUE y del TEDH, a la hora de establecer limitaciones a un derecho fundamental deben tenerse en cuenta una serie de criterios, en concreto: que la limitación haya sido establecida por ley, que respete el contenido esencial del derecho o libertad, que sea necesaria, que responda efectivamente a objetivos de interés general reconocidos por la Unión o por la necesidad de protección de los derechos y libertades de los demás, y que se respete el principio de proporcionalidad[81]. Y, respeto del análisis del respeto del principio de proporcionalidad, han de tenerse en cuenta asimismo los tres requisitos que el TEDH examina en todo caso para valorar si la injerencia en un derecho fundamental respeta dicho principio: que la injerencia esté prevista por la ley; que atienda a un fin o fines legítimos; y que sea necesaria en una sociedad democrática para el logro de dicho fin o fines[82]. Pues bien, atendiendo a esta jurisprudencia el tenor literal del considerando 56, así como los tenores literales del art. 6.1.e y f, y del art. 9.2.g del RGPD, no cumplirían ninguno de estos requisitos:

1) No reúnen los requisitos de *previsibilidad y accesibilidad*, pues no basta con que la restricción o limitación en el ejercicio de un derecho o libertad haya sido prevista por ley[83], sino que como ha señalado el TEDH deben cumplirse además una serie de exigencias relacionadas con la calidad de la ley[84], en concreto, su previsibilidad y accesibilidad, es decir, la ley debe estar formulada «con la suficiente precisión como para permitir al justiciable ajustar su conducta»[85].

2) Tampoco establecen las *garantías adecuadas* que aseguren el respeto del contenido esencial del derecho, pues como ha señalado el TJUE, además de que la norma establezca reglas claras y precisas que regulen el alcance de la injerencia, son necesarias estas garantías para permitir una protección eficaz de los datos de carácter personal frente a los riesgos de abuso, así como frente a cualquier acceso o utilización ilícitos de los mismos[86]. Si no se establecen esas garantías, incluso aunque un régimen normativo autori-

---

[81] Sobre la aplicación de estos criterios a la protección de datos personales, puede consultarse el análisis realizado por el SEPD. «*Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*», 11 April 2017, Supervisor Europeo de Protección de Datos, 4 y ss.

[82] TEDH (Pleno), caso *Observer y Guardian c. Reino Unido*, 26 de noviembre de 1991, ap. 49.

[83] Toda injerencia o restricción requiere de habilitación legal. TEDH (Pleno), caso *Observer y Guardian c. Reino Unido*, *op. cit.*, ap. 49; TEDH (Gran Sala), caso *Rekvényi c. Hungría*, 20 de mayo de 1999, ap. 34. Y, efectivamente, este punto se cumplía por el art. 58bis.1, que respetaba así lo previsto por los arts. 53.1 y 81.1 de la CE, y por el 9.2 de la LOPDGDD.

[84] TEDH (Gran Sala), caso *Maestri c. Italia*, 17 de febrero de 2004, ap. 30.

[85] TEDH (Gran Sala), caso *Hashman y Harrup c. Reino Unido*, 25 de noviembre de 1999, ap. 31, TEDH (Gran Sala), caso *Rekvényi c. Hungría*, 20 de mayo de 1999, ap. 34.

[86] STJUE de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, *Digital Righst Ireland Ltd*, ap. 54.

zase la recogida de datos con fines legítimos, se vulneraría el derecho a la intimidad[87].

3) Y no determinan la finalidad del tratamiento de los datos, pues no determina qué debe entenderse por ese «interés público» que legitime la restricción del derecho fundamental. Atendiendo tanto a la jurisprudencia del TJUE[88] como del TC, la existencia de un interés general o público no es suficiente, por sí sola, para justificar la medida restrictiva. Una mera invocación genérica, indeterminada, es incompatible con las exigencias de reserva legal pues constituye una cesión en blanco del poder normativo[89]. Como señala el TEDH, «en las cuestiones que afectan a derechos fundamentales, sería contrario al Estado de Derecho [...] que una discrecionalidad legal concedida al ejecutivo se expresara en términos de un poder sin restricciones», por lo tanto, la ley «debe indicar con suficiente claridad el alcance de dicha discrecionalidad y la forma de ejercerla»[90].

Todo esto queda postergados al desarrollo bien por el Derecho de la Unión, bien por los Estados miembros, lo que en este segundo supuesto plantea mayores problemas ya que puede resultar en amplias diferencias entre las legislaciones de estos en un ámbito, las categorías de datos especialmente sensibles, en el que en teoría la protección debería ser máxima[91].

Por otra parte, también debe tenerse en cuenta lo dispuesto en los artículos 13 y 14 del Reglamento, relativos a la información que debe facilitarse tanto cuando los datos se han obtenido del interesado como cuando no se han obtenido de este. Las obligaciones de transparencia que recogen se aplican a todas las categorías de datos, también los especiales, e independientemente de la base para su tratamiento[92]. Porque, tal y como se ha examinado, precisamente la falta de transparencia está detrás de la forma en la que operan las técnicas de *microtargeting* electoral y de difusión de desinformación[93].

---

[87] SSTC 254/1993, de 20 de julio, FJ 4; 143/1994, de 9 de mayo, FJ 7; y 292/200, de 30 de noviembre, FJ 10.

[88] *Ibid.*, ap. 51.

[89] STC 292/2000, de 30 de noviembre, FJ 18.

[90] TEDH (Gran Sala), caso *Maestri c. Italia*, 17 de febrero de 2004, ap. 30.

[91] Además, choca con lo que es el propósito de un Reglamento, buscar una regulación uniforme a nivel de la UE y reducir las diferencias entre los Estados miembros, tal y como destaca el análisis realizado por European Digital Rights EDRI, «Proceed with caution: Flexibilities in the General Data Protection Regulation», 5 July 2016, pp. 2-3. Maeve McDonagh, «Freedom of processing of personal data», 126.

[92] Si bien, con respecto al artículo 14, se critica también la excepción para su no aplicación cuando la comunicación de la información que contempla suponga un esfuerzo desproporcionado o resulte imposible; los problemas que plantea su aplicación en el contexto de las prácticas de *microtargeting* electoral, en las que precisamente los datos se obtienen infiriéndolos de otros que sí ha proporcionado el usuario; y que también los Estados miembros pueda establecer excepciones que hagan diferente la regulación entre ellos. *Ibid.* pp. 137-138.

[93] *Ibid.* pp. 127-129.

En cuanto a la elaboración de perfiles ideológicos, el RGPD garantiza el derecho del interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado —incluida esa elaboración de perfiles— (art. 22.1 RGPD)[94], pero recoge al mismo tiempo las situaciones en las que no se aplicará esta previsión: que la decisión basada en ese tratamiento automatizado sea necesaria para la celebración o ejecución de un contrato entre el interesado y el responsable del tratamiento; que la misma esté autorizada por el Derecho de la Unión o de los Estados miembros, siempre que se establezcan medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o que se base en el consentimiento explícito del interesado (art. 22.2 RGPD)[95]. En el primer y tercer supuesto, el responsable del tratamiento debe adoptar las medidas adecuadas para salvaguardar los derechos e intereses legítimos del interesado y, como mínimo, su derecho a «obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión» (art. 22.3 RGPD)[96]. Y la elaboración de perfiles exige también, de acuerdo con el Reglamento Europeo, su comunicación a los sujetos interesados (art. 13.2.f RGPD).

---

[94] El Tribunal de Justicia ha tenido la oportunidad de interpretar el artículo 22 del RGPD en una sentencia de 2023, señalando que el art. 22.1 consagra un "«derecho» del interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles", disposición que «establece una prohibición de principio cuya inobservancia no necesita ser invocada proactivamente por el interesado». STJUE de 7 de diciembre de 2023, *OQ y Land Hessen*, asunto C-634/21, ap. 52 (más conocida como caso Schufa). Destaca el tribunal que todos los requisitos más estrictos que se establecen para la licitud de una toma de decisiones automatizada, así como las obligaciones adicionales de información del responsable del tratamiento y los derechos de acceso del interesado, se explican por la finalidad que persigue el art. 22, que es «proteger a las personas contra los riesgos específicos para sus derechos y libertades que supone el tratamiento automatizado de datos personales, incluida la elaboración de perfiles». *Ibid.* ap. 57. Como en estos casos el tratamiento implica evaluar aspectos personales para analizar o predecir aspectos relacionados con su situación económica, salud, preferencias, etc., y tiene el riesgo de incidir en los derechos del interesado, con potenciales efectos discriminatorios por motivos de raza, opiniones políticas, religión, etc., señala el TJUE que «es importante establecer garantías adecuadas y garantizar un tratamiento leal y transparente respecto del interesado, en particular mediante la utilización de procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles y la aplicación de medidas técnicas y organizativas apropiadas para garantizar que se reduce al máximo el riesgo de error». *Ibid.* apdos. 58-59. Sobre decisiones automatizadas y scoring, véase también la STJUE de 27 de febrero de 2025, *CK y Magistrat der Stad Wien*, asunto C-203/22.

[95] Estas decisiones no se basarán en las categorías especiales de datos del artículo 9, salvo que se cuente con el consentimiento explícito del interesado (art. 9.2.a)) o su tratamiento sea necesario por razones de interés público esencial (art. 9.2.g)) y se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. Art. 22.3 RGPD.

[96] Sobre el responsable del tratamiento de datos, *vid.* Ignacio Álvarez Rodríguez, «Responsable y Encargado del Tratamiento» en VVAA, *Comentarios a la Nueva Ley de Protección de Datos* (Madrid: Dilex, 2020), 105-125.

Por lo tanto, las técnicas de *microtargeting* electoral deben respetar lo dispuesto por el RGPD, si bien la aplicación en la práctica de estas disposiciones se encuentra con diversos obstáculos. Tal y como señalan Blasi y Vermeulen, el *microtargeting* político plantea una serie de cuestiones relacionadas con alguno de los principios establecidos en el artículo 5 del RGPD:

— Licitud, lealtad y transparencia del tratamiento (art. 5.1.a RGPD). A este respecto, señalan que no siempre es fácil identificar quién es el responsable del tratamiento[97] y que, una vez identificado, tampoco es claro si se ha obtenido el consentimiento válidamente antes del tratamiento[98]. Y como explica el Grupo de Trabajo del Artículo 29, el proceso de elaboración de perfiles suele ser invisible para el interesado y funciona creando datos personales nuevos a través de otros que no han sido facilitados directamente por el interesado[99]. En esos casos el RGPD exige que se facilite a estos información concisa, transparente, inteligible y de fácil acceso (art. 12 RGPD)[100] , lo que no siempre ocurre en el caso de plataformas como Facebook[101].

---

[97] Ha de tenerse en cuenta que en el *microtargeting* electoral intervienen varios actores, no solo los partidos políticos sino también las plataformas, empresas de análisis especializadas, brokers de datos, etc. Se ha planteado si el responsable del tratamiento es solo el partido político que dispone de los datos, o también plataformas como Facebook que ofrece las herramientas de segmentación de audiencias. Tanto el TJUE como las autoridades nacionales de protección de datos, entienden que ambos deben ser considerados responsables del tratamiento. Blasi Casagra y Vermueulen, «Reflections on the murky legal practices», 352.

[98] Porque, señalan, en el caso del *microtargeting* electoral a menudo el usuario no es consciente de que sus datos se están recopilando para un uso específico —tratamiento invisible—. Las herramientas de segmentación entienden que no cumplen los criterios de transparencia e información exigidos por el RGPD, puesto que el consentimiento para esta recopilación de datos suele estar mezclado con los términos y condiciones de la plataforma, lo que hace difícil que se cumpla el requisito de que sea un consentimiento libre, específico, informado y sin ambigüedades. Así, señalan cómo los usuarios de Facebook solo pueden retirar parcialmente el consentimiento a ser sujetos a *microtargeting* (por ejemplo, si pueden oponerse a que el anunciante les incluya en una lista, pero no a que se les seleccione en función de ciertas características como género, edad, etc), pero no a *microtargeting* electoral, es decir, oponerse a que los partidos políticos les envíen anuncios. *Ibid.* p. 354.

[99] «Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679», adoptadas el 3 de octubre de 2017, SP251rev.01, Grupo De Trabajo Sobre Protección De Datos Del Artículo 29, 10.

[100] Como señala el Grupo de trabajo del artículo 29, los responsables del tratamiento deberán demostrar que los interesados entienden exactamente qué están consintiendo, para lo que deberán garantizar que explican de forma clara y sencilla cómo funciona la elaboración de perfiles o las decisiones automatizadas, obligación que deriva del derecho a ser informado que tiene el interesado. *Ibid.* 14 y 18.

[101] Blasi Casagra y Vermueulen, «Reflections on the murky legal practices» 354. McDounagh también destaca las dudas que se han planteado respecto al uso del consentimiento como la base para el tratamiento de datos, especialmente en la era del big data, destacando no solo la complejidad de los acuerdos para dar el consentimiento, sino también la posición de claro desequilibrio entre el usuario y las grandes plataformas que redactan las cláusulas a su favor y de forma que no son negociables pues

— Tratamiento con fines determinados, explícitos y legítimos (art. 5.1.b RGPD) que, en el caso del *microtargeting* electoral, señalan los autores que debería restringirse pues se están utilizando unos datos recogidos a través de plataformas para otra finalidad originalmente [102].

— Minimización de datos, es decir, que los datos tratados sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (art. 5.1.c RGPD). En las prácticas de *microtargeting* electoral se utilizan una gran cantidad de datos, que la plataforma selecciona aplicando una serie de herramientas de análisis, y pone a disposición de los partidos políticos. Pero el número y tipo de datos que se utilizan y combinan no se da a conocer completamente por estas plataformas, por lo que los autores señalan que se estaría infringiendo este principio de minimización [103].

— Exactitud de los datos (art. 5.1.d RGPD), en todas las fases del proceso de elaboración de perfiles (al recoger datos, analizarlos, crear un perfil para una persona, y aplicar un perfil para tomar una decisión que afecta a una persona), lo que señala el Grupo de Trabajo del Artículo 29 «refuerza la importancia de ofrecer una información clara sobre los datos personales que se procesan» [104].

— Responsabilidad proactiva (art. 5.2 RGPD), el responsable del tratamiento será responsable de cumplir los principios fijados en el art. 5.1 del

---

o bien se aceptan por el usuario, o no se recibe el servicio. McDonagh, «Freedom of processing of personal data», 119.

[102] Blasi Casagra y Vermueulen, «Reflections on the murky legal practices», 355. En los casos en que el tratamiento se lleva a cabo para otro fin distinto de aquel para el que se recogieron los datos personales, y no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos del art. 23 del RGPD, el art. 6.4 de este señala que el responsable del tratamiento tendrá que tener en cuenta una serie de factores, como la relación entre los fines para los que se recogieron los datos y los fines del tratamiento ulterior, el contexto en el que se han recogido los datos, la naturaleza de estos, las posibles consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas. Como se ha señalado, en el *microtargeting* electoral es dudoso que el consentimiento se haya obtenido válidamente cumpliendo con lo requerido por el RGPD, por cómo están redactados los términos y condiciones de las plataformas. Y también es dudoso que el responsable del tratamiento en estos casos observe lo previsto en el mencionado art. 6.4 del Reglamento.

[103] Señalan Blasi y Vermeulen en su trabajo que hay estudios que han demostrado que es posible en Facebook combinar criterios que cuadren solo con un individuo y que, por lo tanto, una campaña publicitaria identifique a ese individuo y adquiera información adicional de este, y que las plataformas tampoco dejan que los usuarios puedan decidir qué datos se usan para publicidad, incluso aunque el usuario haya seleccionado las opciones «solo amigos» o «solo yo» hay estudios que han demostrado que se ha podido obtener esa información. Blasi Casagra y Vermueulen, «Reflections on the murky legal practices», 357-358.

[104] «Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679», 13.

RGPD y capaz de demostrarlo. Principio que tampoco se está respetando según los autores pues no hay una información transparente por parte de las plataformas por lo que respecta a los tipos de datos que se utilizan, su número y, sobre todo, los algoritmos que emplean para segmentar las audiencias y enviar la publicidad personalizada [105].

Pero, además, como ha señalado el Comité Europeo de Protección de Datos en su Declaración 2/2019, cuando se tratan datos personales en el transcurso de las actividades electorales deben respetarse una serie de puntos clave [106]:

— Aunque los datos que los votantes individuales hayan hecho públicos o compartido de otro modo no sean datos que revelen opiniones políticas, siguen estando sujetos y protegidos por la legislación en materia de protección de datos y su tratamiento debe cumplir con las obligaciones relativas a la transparencia, la finalidad y la legalidad. Efectivamente, puede que a través de las plataformas o redes sociales no se revele directamente la opinión política, pero que a través de otra información (noticias compartidas, *likes* a otras publicaciones, etc.) si se puede saber indirectamente cuál puede ser la ideología de una persona por lo que, como señalan Cristina Blasi y Mathias Vermeulen, podría argumentarse que las prácticas de *microtargeting* electoral deberían considerarse como sensibles y exigir a los actores políticos obtener el consentimiento explícito previo del interesado [107].

— Incluso cuando el tratamiento es legal, deben cumplirse las demás obligaciones establecidas en el RGPD «incluido el deber de transparencia y facilitar información suficiente a las personas que se están analizando y cuyos datos personales se tratan» [108].

— Solo se restringe la toma de decisiones automatizada, incluida la elaboración de perfiles, en la que la decisión afecta significativamente al individuo objeto de esta; añadiendo que, en determinadas circunstancias, la elaboración de perfiles relacionados con la mensajería de campaña selectiva «puede provocar «efectos igualmente significativos» y, en principio, solo será legal con el consentimiento explícito válido del interesado» [109].

— Y que, en caso de selección, se ha de facilitar la información adecuada a los votantes, explicándoles por qué están recibiendo un determinado mensaje, quién es el responsable del mismo y cómo pueden ejercer sus derechos como interesados [110].

Asimismo, como recuerda el Comité, el respeto a las disposiciones del RGPD y la sujeción a la supervisión de las autoridades independientes encar-

---

105 Blasi Casagra y Vermueulen, «Reflections on the murky legal practices», p. 357.

106 Comité Europeo De Protección De Datos, 2-3.

107 Blasi Casagra y Vermueulen, «Reflections on the murky legal practices», 354-355.

108 Comité Europeo De Protección De Datos, 2.

109 *Ibid.* pp. 2-3.

110 *Ibid.* p. 3.

gadas de la protección de datos no sólo se predica de los partidos políticos y candidatos, sino también de otros agentes que pueden participar en el tratamiento de datos personales con fines políticos (redes sociales, grupos de interés, agentes de datos, empresas de análisis y redes ad hoc), pues también estos pueden desempeñar un papel importante en el proceso electoral[111].

En resumen, aunque el tratamiento de datos personales relativos a las opiniones políticas de las personas, especialmente en el marco de las actividades electorales, queda cubierto por el RGPD, su aplicación práctica es problemática y encuentra numerosos obstáculos, a lo que no contribuye que en las disposiciones analizadas se permita que los Estados miembros puedan introducir excepciones a lo dispuesto en la norma europea, lo que afecta a la uniformidad que se busca con este tipo de norma[112]. Como señala Hernández Peña, si bien el Reglamento refuerza la protección de datos, con respecto al perfilado ideológico y el *microtargeting* es una regulación inacabada[113]. Por ello, entendemos que la reciente normativa de la UE que se examina en los siguientes apartados aborda alguno de estos problemas, y aunque no desplaza al RGPD si puede ayudar a reforzar la protección de los usuarios, especialmente al incrementar las obligaciones de transparencia de las plataformas con respecto al uso que realizan de los datos de sus usuarios y de sus sistemas de recomendaciones, así como para regular cómo debe realizarse la segmentación de la publicidad política.

4.2. El Reglamento de Transparencia y Segmentación de la publicidad política

El Reglamento de transparencia y segmentación de la publicidad política fue aprobado por el Parlamento Europeo y el Consejo el 13 de marzo de 2024, y tiene por objetivo garantizar que la prestación de los servicios de publicidad política respete los derechos fundamentales. Como claramente explica el Reglamento en su exposición de motivos, la publicidad política puede ser un vector de desinformación, especialmente cuando no revela su naturaleza política, proviene de patrocinadores de fuera de la Unión o está sujeta a técnicas de segmentación basadas en el tratamiento de datos personales, en particular datos inferidos, como son los que revelan las opiniones políticas de las personas. Por ello, es necesario garantizar un nivel elevado de transparencia, que posibilite un debate y unas campañas políticas abiertas y justas, unas elecciones o referendos libres y justos, y contrarrestar la manipulación de la información y las inferencias ilícitas, también las que provienen de terceros países[114].

---

111 *Ibid.* p. 2.

112 McDonagh, «Freedom of processing of personal data», 138.

113 Hernández Peña, «Campañas electorales», 51 y ss.

114 Considerandos 4, 5 y 6 del Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política. *DOUE* nº 900, de 20 de marzo de 2024 (en adelante, RTSPP)

El legislador europeo adopta este Reglamento debido a que la regulación de la publicidad política era heterogénea a nivel de los Estados miembros y solía centrarse en las formas tradicionales de los medios de comunicación, y porque se trata de un ámbito en el que entronca con la prestación de servicios y el mercado interior, por lo que era necesario garantizar en la Unión un nivel de transparencia coherente y elevado en la publicidad política, evitando divergencias que obstaculicen la libre prestación de servicios de publicidad política[115].

Las nuevas reglas abarcan las normas armonizadas para la prestación de servicios de publicidad política y servicios conexos, incluidas las obligaciones de transparencia, las normas armonizadas sobre el uso de técnicas de segmentación que impliquen el tratamiento de datos personales, y las normas sobre la supervisión y ejecución del Reglamento[116]. No afectan al contenido de los anuncios, ni a otros aspectos como la realización de las campañas, que siguen sujetos a la legislación nacional[117].

Por lo que respecta a la transparencia de la publicidad política, el Reglamento recoge una serie de obligaciones para los prestadores de servicios publicitarios que deben identificar claramente la publicidad política mediante una etiqueta de transparencia para cada anuncio político que deberá incluir una declaración de que se trata de un anuncio político; la identidad de su patrocinador y, en su caso, de la entidad que en última instancia controla al patrocinador; en su caso, las elecciones, el referéndum o el proceso legislativo a que está vinculando el anuncio político; en su caso, una declaración de que se han aplicado al anuncio técnicas de segmentación o de entrega de anuncios; y un aviso de transparencia que contenga la información que requiere el Reglamento o una indicación clara del lugar en que puede consultarse[118]. De esta forma, será posible conocer quién está detrás de ese anuncio, que financiación ha recibido, y si se han utilizado técnicas de segmentación para la difusión de este.

En cuanto a las técnicas de segmentación y de entrega de anuncios, tendrán que explicarse detalladamente y quedan sujetas a unos requisitos específicos, permitiendo solo las técnicas de segmentación que impliquen el tratamiento de datos personales si el interesado ha proporcionado dichos datos, ha dado su consentimiento expreso, y si dichas técnicas no implican una elaboración de perfiles tal y como se define en el RGPD utilizando las categorías especiales de datos a que este hace referencia. Por lo tanto, a sensu contrario, quedan prohibidas cuando impliquen la elaboración de perfiles que utilicen datos sensibles, o cuando se realicen sin el consentimiento expreso de la persona interesada[119].

---

115 *Ibid.* considerandos 7 y ss y artículo 1 RTSPP.

116 *Ibid.* artículo 1 RTSPP.

117 «La UE introduce nuevas normas sobre transparencia y segmentación en la publicidad política», Consejo De La Unión Europea.

118 Art. 11 RTSPP.

119 *Ibid.* art. 18 RTSPP.

Además, se establecen una serie de requisitos adicionales, además de los requisitos específicos y de los que establece el RGPD, en virtud de los cuales los responsables del tratamiento tendrán que cumplir otra serie de requisitos [120]:

— Adoptar, aplicar y hacer pública una política interna que describa con claridad y en un lenguaje sencillo cómo se usan dichas técnicas para segmentar, y mantener dicha política durante siete años.

— Mantener registros del uso de dichas técnicas, los mecanismos y parámetros pertinentes utilizados.

— Proporcionar, junto con la indicación de que es un anuncio político, la información adicional necesaria para que la persona interesada pueda comprender la lógica aplicada y los principales parámetros de las técnicas utilizadas, incluyendo si se han utilizado técnicas de IA para orientar o entregar el anuncio, así como una serie de elementos como las categorías de datos personales utilizados, los grupos específicos de destinatarios objetivo junto con los parámetros usados para determinar los mismos, o los objetivos, mecanismos y lógica de la segmentación, incluidos los parámetros de inclusión y exclusión y las razones para elegir estos parámetros.

También supone una mejora que se requiere que el interesado haya dado, por separado, su consentimiento expreso para el tratamiento de sus datos, que se tenga que asegurar que las técnicas de segmentación no impliquen la elaboración de perfiles utilizando las categorías especiales de datos (si bien no se impide que se pueda hacer ese perfilado infiriendo esos datos de otros que sí ha proporcionado el usuario), que no se pueda solicitar el consentimiento del interesado si este ya ha indicado por medios automatizados que no presta su consentimiento al tratamiento de sus datos con fines de publicidad política, y que se ofrezca al interesado que no haya dado su consentimiento una alternativa equivalente para que pueda utilizar el servicio en línea sin recibir la publicidad política [121].

Ahora bien, una de las enmiendas presentadas por el Parlamento Europeo a la propuesta de la Comisión durante la tramitación legislativa, buscaba endurecer las disposiciones sobre segmentación y publicidad política en línea [122], contemplando que «los datos personales facilitados por el interesado debido al uso de un servicio o dispositivo, incluido el contenido facilitado, no se considerarán datos personales facilitados y, por tanto, no serán utilizados por el proveedor a efectos de segmentación y entrega de publicidad política» [123]; que «cuando solicite el consentimiento del interesado, el responsable del trata-

---

120 *Ibid.* art. 19 RTSPP.

121 *Ibid.* art. 18 RTSPP.

122 María Díaz Crego, *Regulación de la publicidad política*. Servicio de Estudios del Parlamento Europeo, PE739.311, enero 2023.

123 Enmienda 207. Enmiendas aprobadas por el Parlamento Europeo el 2 de febrero de 2023 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la transparencia y la segmentación de la publicidad política (COM(2021)0731 – C9-0433/2021 – 2021/0381(COD)). P9_TA(2023)0027.

miento informará de que sus datos personales facilitados podrán ser tratados únicamente con el fin de presentar publicidad política al interesado» y que «la denegación del consentimiento no resultará al interesado más difícil que su concesión, ni le requerirá más tiempo» [124]; y que las técnicas de segmentación y entrega de anuncios no combinarán «más de cuatro categorías de datos personales, incluida la ubicación del interesado» [125]. La enmienda era mucho más ambiciosa y habría sido preferible, pues reforzaba mucho más la protección de los usuarios e imponía más restricciones a la segmentación al limitar a cuatro categorías de datos como máximo para combinar e introducir restricciones geográficas para la segmentación, entre otros elementos. Habría servido, de haber sido aprobada, para evitar una microsegmentación excesiva, lo que habría contribuido mucho más a luchar contra las técnicas de manipulación y desinformación, garantizando mucho más los derechos de los ciudadanos.

Por último, para contrarrestar la injerencia en las elecciones por parte de determinadas entidades de terceros países, o nacionales de terceros países, el Reglamento prevé que en los tres meses anteriores a una elección o un referéndum organizados a escala de la Unión o a nivel nacional, regional o local en un Estado miembro, los prestadores de servicios de publicidad política deben estar obligados a prestar servicios de publicidad política únicamente a ciudadanos de la Unión, nacionales de terceros países que residan permanentemente en la Unión y tengan derecho de voto en dichas elecciones o referendos, o a personas jurídicas establecidas en la Unión que no estén controladas por entidades de terceros países [126].

En resumen, el nuevo Reglamento armoniza las normas en esta materia para reforzar la transparencia de la publicidad política, permitir que pueda conocerse quién está detrás de ella, regular el uso de técnicas de segmentación y prohibir la utilización de datos sensibles en dichas técnicas, como los datos relativos a las opiniones políticas de las personas, por lo que contribuye a luchar contra las prácticas indebidas de *microtargeting* electoral. Ahora bien, con respecto a las técnicas de segmentación como se ha señalado la enmienda presentada por el Parlamento Europeo habría sido preferible al ser mucho más garantista.

4.3. Otras normas de la UE que se pueden aplicar a las prácticas de *microtargeting* electoral

El presente apartado tiene por objeto examinar otras normas adoptadas recientemente a nivel de la Unión Europea que, en el marco del funcionamiento del mercado interior, contienen disposiciones que se aplican a la protección de datos personales y a las técnicas de *microtargeting* electoral, y con-

124 *Ibid.*
125 *Ibid.*
126 Considerando 19 y artículo 5.2.c. RTSPP.

tribuyen a regular el uso correcto de las nuevas tecnologías y limitar el uso indebido de estas, como arma de difusión de desinformación y manipulación de los procesos electorales. Así, se examinarán el Reglamento de Inteligencia Artificial, los Reglamentos de servicios y mercados digitales y el Reglamento de transparencia y segmentación de la publicidad política[127].

4.3.1. El Reglamento de Inteligencia Artificial.

Como bien señala María Garrote de Marcos, la capacidad actual de la IA para producir *deepfakes*, lanzar ciberataques y difundir desinformación no puede despreciarse y, como se viene apuntando, puede «desestabilizar los procesos democráticos, amenazar la integridad del discurso político y erosionar la confianza pública»[128]. Por ello, es conveniente analizar si el nuevo Reglamento de Inteligencia Artificial puede contribuir a hacer frente a alguno de estos riesgos.

De acuerdo con el artículo 1 del Reglamento su objetivo es «mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA (en lo sucesivo, "sistemas de IA") en la Unión así como prestar apoyo a la innovación»[129].

En el contexto del *microtargeting* electoral, los sistemas de IA que se utilicen para realizar estas prácticas y personalizar los mensajes a enviar a individuos o grupos específicos quedarían sujetos a las disposiciones del Reglamento relativas a la clasificación de este tipo de sistemas en función del riesgo, así:

---

[127] A ellos podría añadirse el Reglamento (UE, Euratom) 2019/493 por el que se establece un procedimiento de verificación relativo a las infracciones de las normas de protección de datos personales que puedan darse en el contexto de las elecciones al Parlamento Europeo, pero ya que su aplicación está limitada a dichas elecciones no realizaremos un análisis en el presente trabajo ya que este se enfoca en las normas que afectan al funcionamiento del mercado interior. El Reglamento crea una Autoridad para los partidos políticos europeos que desempeñará funciones de protección de la integridad del proceso electoral en condiciones de neutralidad, y podrá imponer sanciones a los partidos que no respeten la protección de datos. Reglamento (UE, Euratom) 2019/493 del Parlamento Europeo y del Consejo de 25 de marzo por el que se modifica el Reglamento (UE, EURATOM) 1141/2014 en lo que respecta a un procedimiento de verificación relativo a las instrucciones de las normas de protección de los datos personales en el contexto de las elecciones al Parlamento Europeo. *DOUE* nº 85, de 27 de marzo de 2019.

[128] Garrote de Marcos, «La IA en el período electoral», 265.

[129] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. *DOUE* nº 1689, de 12 de junio de 2024 (en adelante, Reglamento IA).

— Quedarán prohibidos por suponer un riesgo inaceptable los sistemas que permitan manipular el comportamiento humano mediante técnicas subliminales con el objetivo de alterar de manera sustancial el comportamiento de una persona o colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, y de forma que provoque, o sería razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas[130]. Como se reconoce en los considerandos del propio Reglamento, los sistemas de IA pueden utilizarse indebidamente y «proporcionar nuevas y poderosas herramientas para llevar a cabo prácticas de manipulación, explotación y control social», prácticas que son incorrectas y deben estar prohibidas[131].

Evidentemente, en estos supuestos la dificultad radica en probar que el sistema está utilizando este tipo de técnicas, por ejemplo, que se ha entrenado con imágenes sesgadas, está segmentando a los electores en función de determinadas opiniones políticas, o presentando información de manera distorsionada para favorecer a un determinado partido político. Pero esto solo es posible si el código del algoritmo es accesible[132], lo que no ocurre con la mayoría de los sistemas de IA actuales[133]. El mismo uso de sistemas de IA podría ayudar a detectar mensajes sesgados o falsos en la publicidad política, incluso el posible uso de algoritmos con patrones de manipulación. Pero la principal dificultad, a nuestro entender, es que habrá que demostrar también que el sistema ha alterado de manera significativa la intención de voto del elector, que de otra forma no habría tomado, así como demostrar que se están produciendo esos perjuicios considerables que señala el Reglamento, lo que es verdaderamente complejo.

— Se considerarán de alto riesgo los sistemas que se utilicen para influir en el resultado de una elección o referéndum, o en el comportamiento electoral de las personas físicas que ejerzan su derecho de voto en elecciones o referéndums[134], por lo que quedan sujetos a una serie de requisitos previstos

---

130 Artículo 5 Reglamento IA.

131 Considerando 28 Reglamento IA.

132 Código del algoritmo es el código escrito, mediante lenguaje de programación, que permite que el programa, página web o sistema de IA funcione y ejecute una tarea determinada. Es decir, es una secuencia de instrucciones que se programa para que el sistema pueda resolver un problema específico. Una definición tanto del término código como de algoritmo puede encontrarse en el Glosario sobre IA disponible en la página web del Instituto de Derecho Parlamentario de la UCM: *https://www.idpucm.com/glosario/*

133 DeepSeek si es de código abierto, por ejemplo, pero no sus rivales como ChatGPT. Irene Modrón Lecue, «¿Qué es el código abierto en el que se basa la IA DeepSeek y cómo contribuye al desarrollo de la tecnología?», *RTVE*, 10 de febrero de 2025. Acceso el 15 de marzo de 2025, *www.elpais.es*

134 Quedan excluidos, de acuerdo con lo dispuesto en el punto 8 del Anexo III del Reglamento «los sistemas de IA a cuyos resultados de salida no estén directamente expuestos las personas físicas, como las herramientas utilizadas para organizar, op-

por el Reglamento, como la implementación de procedimientos para identificar y mitigar riesgos asociados a su uso, o el mantenimiento de registros detallados para evaluar su conformidad con el Reglamento[135].

Por otra parte, el Reglamento también enfatiza la protección de los datos personales que sean utilizados por los sistemas de IA, protección que debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA, recordando que son aplicables los principios de minimización de datos y de protección de datos desde el diseño y por defecto, tal y como vienen establecidos por la normativa europea en materia de protección de datos[136].

En todo caso, conforme al Reglamento los desarrolladores y proveedores de sistemas de IA de alto riesgo quedan sujetos a una serie de obligaciones, debiendo velar por el cumplimiento de los requisitos de este tipo de sistemas, adoptar medidas correctoras cuando consideren o tengan motivos para considerar que un sistema de alto riesgo no es conforme con el Reglamento, cooperar con las autoridades competentes para demostrar la conformidad de estos sistemas con los requisitos previstos en el Reglamento, etc.[137]. Así, la UE refuerza su marco legal y exige mayor transparencia, contemplando la posibilidad del establecimiento de sanciones por parte de los Estados miembros para los casos en que se infrinja el Reglamento[138].

Ahora bien, el Reglamento también puede encontrar sus limitaciones en la posibilidad de supervisar que los desarrolladores y proveedores cumplan con las obligaciones establecidas. Así, por ejemplo, Elsa Arnaiz critica que los deepfakes —que ya se están utilizando incluso por partidos políticos— se clasifican generalmente como de riesgo limitado y que las obligaciones de transparencia —etiquetado con marca de agua— son fácilmente eludibles[139].

4.3.2. Los Reglamentos de Servicios y Mercados Digitales.

Como señala Miryam Rodríguez Izquierdo, también es necesario que quienes operan en el mercado digital y ofrecen servicios de intermediación estén sujetos a una serie de obligaciones, de forma que los consumidores y usuarios queden también protegidos[140].

---

timizar o estructurar campañas políticas desde un punto de vista administrativo o logístico». ANEXO III Reglamento IA.

135 Artículos 8 a 15 Reglamento IA.

136 Considerando 69 Reglamento IA.

137 Arts. 16 y ss Reglamento IA.

138 Art. 99 Reglamento IA.

139 Elsa Arnaiz Chico, «El colapso del ágora digital: como la IA generativa está enterrando la democracia». *El País*, marzo 2025. Acceso el 15 de marzo de 2025, *www.elpais.es*.

140 Rodríguez-Izquierdo, «El mercado interior», 3.

En primer lugar, encontramos el Reglamento de Servicios Digitales (más comúnmente conocido como Ley de Servicios Digitales)[141], del que pueden destacarse una serie de disposiciones que son aplicables a las prácticas de *microtargeting* electoral, si bien sólo hacen referencia a los prestadores de plataformas en línea[142] y motores de búsqueda de muy gran tamaño (VLOP y VLOSE respectivamente, que implica que tienen más de 45 millones de usuarios)[143]:

— En primer lugar, las disposiciones relativas a la transparencia de la publicidad en línea, que obligan a las plataformas y motores de búsqueda en línea señalados a recopilar y hacer público en sus interfaces en línea un repositorio con toda una serie de información (contenido del anuncio, persona física o jurídica en cuyo nombre se presenta, etc) durante todo el tiempo en que presenten el anuncio y hasta un año después de la última vez que este se presente en sus interfaces[144]. De esta forma, garantizando la transparencia se podrá saber quiénes están detrás de los mensajes publicitarios en general y, en particular, también de la publicidad política.

— En segundo lugar, las disposiciones que obligan a los prestadores de servicios intermediarios señalados a evaluar los riesgos sistémicos que entraña el diseño, funcionamiento y uso de sus servicios, así como los posibles usos indebidos por parte de los destinatarios de estos servicios. En concreto, deben evaluar cuatro categorías de riesgos sistémicos, siendo una de ellas los efectos reales o previsibles del servicio para el ejercicio de los derechos fundamentales, entre los que se enumeran la libertad de expresión y de información, la libertad de medios de comunicación y su pluralismo[145], derechos todos ellos que como se ha examinado anteriormente juegan un papel fun-

---

[141] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales. *DOUE* nº 277, de 27 de octubre de 2022 (en adelante, LSD, acrónimo de Ley de Servicios Digitales, como se conoce al Reglamento).

[142] Plataformas en línea, de acuerdo con la LSD, son los servicios de alojamiento de datos que almacenan y difunden información al público, a petición de un destinatario del servicio «salvo que esa actividad sea una característica menor y puramente auxiliar de otro servicio o una funcionalidad menor del servicio principal y que no pueda utilizarse sin ese otro servicio por razones objetivas y técnicas, y que la integración de la característica o funcionalidad en el otro servicio no sea un medio para eludir la aplicabilidad del presente Reglamento». *Ibid.* artículo 3.i) LSD. Así, por ejemplo, Amazon Services Europe S.à.r.l. Las plataformas en línea que han sido designadas por la Comisión Euorpea como de muy gran tamaño pueden consultarse aquí: *https://digital-strategy.ec.europa.eu/es/policies/list-designated-vlops-and-vloses*

[143] Motor de búsqueda en línea, conforme a la LSD, es un servicio intermediario que permite a los usuarios introducir consultas para hacer búsquedas en cualq uier sitio web. Artículo 3.j) LSD. Así, por ejemplo, Google Irland Ltd. Dichos motores también pueden consultarse en *https://digital-strategy.ec.europa.eu/es/policies/list-designated-vlops-and-vloses*

[144] Artículo 39 LSD.

[145] *Ibid* Considerandos 79-80 y artículo 34 LSD.

damental en toda contienda electoral y pueden quedar afectados por el uso indebido de técnicas de *microtargeting* electoral; así como los riesgos sistémicos que tengan cualquier efecto negativo real o previsible sobre el discurso cívico y los procesos electorales[146]. Además, deben tomar medidas proactivas que reduzcan los riesgos de forma razonable, sean proporcionadas y efectivas[147], y someterse, al menos una vez al año, a auditorías independientes para evaluar el cumplimiento de estas obligaciones[148]. Por lo tanto, puede decirse que las plataformas y motores de búsqueda deben identificar estos riesgos sistémicos también durante los procesos electorales y adoptar medidas que prevengan el uso de sus servicios en campañas de *microtargeting* electoral fraudulentas que pretendan alterar la integridad del proceso electoral mediante la difusión de desinformación[149]. El principal problema que puede plantear esta regulación es que queda en manos de las compañías realizar la evaluación señalada, pero en todo caso debe ajustarse a lo dispuesto en el Reglamento y están sujetas a auditorías independientes.

El Reglamento también recoge obligaciones de transparencia informativa para todos los prestadores de servicios intermediarios, que deberán publicar al menos una vez al año informes sobre las actividades de moderación de contenidos que hayan realizado, así como la información que tendrán que proporcionar aquellos prestadores de plataformas en línea que presenten anuncios publicitarios en sus interfaces (que deberán informar no solo de quien publica el anuncio sino también de los parámetros utilizados para segmentar las audiencias, y dar opción al destinatario para cambiar esos parámetros), y las obligaciones de transparencia de los sistemas de recomendación que utilicen[150]. Por lo tanto, también de esta forma se podrá saber quién está detrás de un anuncio político que no se haya publicado en grandes plataformas y se podrá realizar una trazabilidad de las actividades de moderación y sistemas de recomendación que pueden permitir luchar contra la manipulación informativa.

En cuanto a la lucha contra la desinformación y la difusión de contenidos ilegales, el Reglamento también contiene disposiciones que buscan mejorar la moderación de contenidos y aumentar la transparencia:

— Mecanismos de notificación y acción: los prestadores de servicios de alojamiento de datos deberán establecer mecanismos que permitan notifi-

---

146 *Ibid.* art. 34.1.c) LSD.

147 *Ibid.* art. 35 LSD.

148 *Ibid.* art. 37 LSD.

149 Como señala Tuset Varela, al requerir a las plataformas que adopten medidas para evitar la propagación de contenido falso o engañoso, se puede proteger la integridad del proceso electoral. Damián Tusset Varela, «Cuando la IA decide: fronteras legales y éticas de la IA en el sistema electoral», *Diario La Ley*, 30/1/2024, VI. Marco regulatorio de la Unión Europea y de España, para. 12. Acceso el 12 de enero de 2025, *https://diariolaley.laleynext.es/dll/2024/02/02/cuando-la-ia-decide-fronteras-legales-y-eticas-de-la-ia-en-el-sistema-electoral*

150 Arts. 15, 26 y 27 LSD.

car la presencia en su servicio de elementos de información concretos que se consideren contenidos ilícitos[151], recogiendo asimismo salvaguardas para prevenir el uso abusivo de estos mecanismos, es decir, de forma que se traten de utilizar para eliminar contenidos totalmente lícitos[152].

— Sistemas internos de reclamaciones: los prestadores también deberán establecer sistemas internos de recurso, que permitan a los usuarios impugnar las decisiones relacionadas con la eliminación de contenidos o suspensión de cuentas, debiendo informar a los usuarios de dichos sistemas[153].

— Colaboración con alertadores fiables: los prestadores también deben colaborar con los alertadores fiables que, de acuerdo con el Reglamento, es una condición es se otorga, previa solicitud, a cualquier entidad que lo desee y que demuestre que poseer conocimientos y competencias específicos para detectar, identificar y notificar contenidos ilícitos, que no depende de ningún prestador de plataformas en línea, y que realiza sus actividades con el fin de enviar notificaciones de manera diligente, precisa y objetiva[154]. Entendemos, por lo tanto, que medios de *fact-checking* podrían solicitar esta condición debido al papel que juegan en la comprobación de informaciones falsas o sesgadas.

— Obligaciones de transparencia en la publicidad y los sistemas de recomendación: como se ha adelantado, se establecen una serie de obligaciones para los prestadores de plataformas en línea en materia de transparencia informativa, en el diseño y organización de sus interfaces, en materia de publicidad, y en la forma en que funcionan sus sistemas de recomendación[155]. Todo ello, contribuye también a limitar la utilización de estas plataformas para la difusión de desinformación.

— Obligaciones de evaluación y mitigación de riesgos: previstas para las plataformas de muy gran tamaño, tal y como se ha adelantado, que incluyen también la difusión de desinformación[156].

Por lo tanto, se trata de esta forma de luchar contra los contenidos ilícitos en línea, mediante un mayor control de lo que ven los usuarios, así como de una mayor información a estos de los anuncios que ven, permitiendo que se identifiquen fácilmente los contenidos ilícitos, los discursos de odio y la desinformación[157].

Por último, el Reglamento también prevé la elaboración de códigos de conducta voluntarios, que contribuyan a la aplicación del Reglamento, y que

---

151 *Ibid* art. 16 LSD.
152 *Ibid.* art. 20 LSD.
153 *Ibid.* arts. 16.5 y 17.2.f) LSD, entre otros.
154 *Ibid.* art. 22 LSD.
155 *Ibid.* arts. 24 a 29 LSD.
156 *Ibid.* art. 26 LSD.
157 «Reglamento de Servicios Digitales», EUR-Lex. Acceso el 13 de marzo de 2025, *https://eur-lex.europa.eu/ES/legal-content/summary/digital-services-act.html.*

sirvan de base para iniciativas de autorregulación, como el Código de buenas prácticas en materia de desinformación que se reforzó en 2022 para ser reconocido como Código de Conducta en virtud del Reglamento[158]. Y las disposiciones relativas al acceso de a los datos de las grandes plataformas y motores de búsqueda por parte de investigadores autorizados, también pueden servir para luchar contra la desinformación al permitir de esta forma que se puedan realizar estudios que puedan supervisar las prácticas de *microtargeting* electoral que las plataformas realizan y la publicidad de información que se envía a través de ellas[159].

En cuanto al Reglamento de Mercados Digitales (más comúnmente conocido como Ley de Mercados Digitales), busca garantizar la competencia legal entre las grandes plataformas digitales (los llamados guardianes de acceso), fijando normas claras para las grandes plataformas a fin de garantizar que no abusen de su posición, y aunque no está dirigido a las prácticas de *microtargeting* electoral y de lucha contra la desinformación algunas de sus disposiciones también podrían ser de aplicación[160]:

— En primer lugar, el Reglamento prohíbe a los guardianes de acceso procesar datos personales de los usuarios con fines de publicidad personalizada, a menos que hayan obtenido el consentimiento del usuario[161]. En concreto, no pueden tratarlos, ni combinarlos con otros datos, ni cruzarlos sin ese consentimiento expreso. Se trata así de dificultar la obtención de datos para las prácticas de *microtargeting* electoral. Ahora bien, ya se ha abordado en el punto 5.1 los problemas que se plantean respecto al consentimiento explícito, por la forma en que se redactan los términos y condiciones de las plataformas y la imposibilidad de negociar por parte del usuario, debiendo aceptar si quiere acceder al servicio.

— En segundo lugar, el Reglamento también prohíbe que los guardianes de acceso clasifiquen sus productos de manera más favorable que los de otras empresas, impidan que los desarrolladores utilicen plataformas de pago de terceros para vender aplicaciones, establezcan condiciones injustas para los usuarios profesionales, e impongan restricciones a dichos usuarios[162]. De esta forma, se trata de evitar que utilicen su posición dominante e impidan otras opciones, lo que traducido al ámbito objeto de nuestro estudio se tra-

---

158 «Código de buenas prácticas en materia de desinformación de 2022», Comisión Europea, acceso el 10 de marzo de 2025, *https://digital-strategy.ec.europa.eu/es/policies/code-practice-disinformation*

159 Art. 40 LSD.

160 Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital. *DOUE* nº 265, de 12 de octubre de 2022 (en adelante, LMD).

161 *Ibid.* artículo 5 LMD.

162 «Reglamento de Mercados Digitales», Consejo Europeo/Consejo De La Unión Europea, acceso el 13 de marzo de 2025, *https://www.consilium.europa.eu/es/policies/digital-markets-act/*

duciría en la ocultación de ciertos tipos de contenido y comunicación[163] para favorecer ciertas opciones políticas[164].

— En tercer lugar, el Reglamento prohíbe pre-instalar determinadas aplicaciones, así como dificultar su desinstalación a los usuarios[165]. De esta forma, los usuarios podrán desinstalar aplicaciones que pueden, a su vez, estar recopilando datos que luego sean utilizados para las prácticas de *microtargeting* electoral.

Por lo tanto, con la combinación de las disposiciones de ambos Reglamentos se logra una mayor transparencia en la publicidad en línea, lo que incluye la publicidad política[166]; un mayor control sobre los servicios digitales que se ofrecen; y se introducen medidas para luchar contra la difusión de contenidos ilícitos y desinformación, que también son aplicables a las prácticas de *microtargeting* electoral y contribuyen a luchar contra un uso indebido de estas.

CONCLUSIONES

En las últimas décadas, el avance de las nuevas tecnologías ha posibilitado un acceso sin precedentes a una gran variedad de información y ampliado las posibilidades de los ciudadanos de involucrarse y expresar sus opiniones durante las campañas electorales. Pero estos avances han venido acompañados de la proliferación de difusión de noticias falsas o sesgadas que tratan de influir en dichas campañas, poniendo en peligro los principios que deben regir toda contienda electoral y afectando a derechos, valores y principios democráticos fundamentales. Los Estados democráticos que hemos alcanzado hace tiempo que no se veían tan amenazados.

La utilización de técnicas de *microtargeting* electoral para segmentar las audiencias a las que dirigir publicidad política de forma personalizada, con el objetivo de aumentar las posibilidades de que se vote a un determinado candidato, sumado a la forma en la que funcionan los sistemas de recomendación de las plataformas —que genera burbujas de filtro—, y a la difusión de desinformación durante las campañas electorales, hacen necesario que se actúe desde el nivel de la Unión para tratar de garantizar la realización de elecciones verdaderamente libres, en las que se respeten los principios de objetividad, neutralidad política, transparencia e igualdad de armas.

---

163 Rodríguez-Izquierdo, «El mercado interior», 10.

164 Tusset Varela, «Cuando la IA decide», VI. Marco regulatorio de la Unión Europea y de España, para. 13.

165 Artículo 6 LMD.

166 Transparencia que es fundamental, señala Tusset Varela, durante las campañas electorales, para que el votante sepa quién está tratando de influir en su opinión. Damián Tusset Varela, «Cuando la IA decide», VI. Marco regulatorio de la Unión Europea y de España, para. 12.

Debido a que para realizar las técnicas de *microtargeting* electoral son necesarios datos personales de los que disponen las plataformas y redes sociales, y a que el envío de información y propaganda política se puede realizar también a través de estas, nos encontramos ante un ámbito en el que los titulares de esas plataformas, como prestadores de servicios o intermediarios, se encuentran actuando en el mercado interior de la Unión Europea. Por lo tanto, la Unión puede utilizar su competencia para establecer normas de competencia relativas al funcionamiento del mercado interior, así como para la protección de los datos personales de sus ciudadanos. Y, efectivamente, en el uso de dicha competencia la Unión Europea ha adoptado en los últimos años importantes Reglamentos que vienen a regular las prácticas de estas plataformas y prestadores de servicios, que se aplican a las técnicas de *microtargeting* electoral y tratan de poner coto a las prácticas de difusión de desinformación.

Como se ha examinado en el presente trabajo, las prácticas de *microtargeting* electoral deben respetar las disposiciones que establece el RGPD, pero la realidad muestra que es verdaderamente complejo comprobar que se respeta los establecido por este. Si bien el Reglamento requiere el consentimiento explícito del interesado para poder tratar sus datos, no solo en numerosas ocasiones es prácticamente imposible comprobar que se ha obtenido dicho consentimiento, sino también que este sea verdaderamente informado. Por una parte, los términos y condiciones que utilizan las plataformas suelen ser excesivamente largos y utilizan terminología no siempre comprensible para cualquier usuario. Por lo tanto, no siempre la información es concisa, transparente, inteligible y de fácil acceso, y cumple con los requisitos de licitud, lealtad y transparencia previstos por el Reglamento. Por otra parte, tampoco se suele cumplir con el requisito de que el tratamiento sea con fines determinados, explícitos y legítimos, pues la elaboración de perfiles funciona utilizando datos recogidos por las plataformas para una finalidad original, para crear nuevos datos para otra finalidad diferente. Lo que infringe también el principio de minimización de datos, pues las prácticas de *microtargeting* electoral utilizan gran cantidad de datos que van más allá de lo necesario en relación con los fines para los que son tratados. Requisitos que deberían respetarse, especialmente cuando se tratan datos personales en el transcurso de las actividades electorales.

Los nuevos Reglamentos de IA, de Servicios y Mercados Digitales, y de transparencia y segmentación de la publicidad política también tratan de abordar estos problemas, de forma que los prestadores de este tipo de servicios queden sujetos a unas obligaciones, con el fin no solo de garantizar la adecuada competencia y funcionamiento del mercado interior, sino también de proteger los derechos fundamentales que los Tratados y la Carta recogen. Son de destacar las disposiciones que exigen mayor transparencia, especialmente las relacionadas con la publicidad en línea, tanto las que contempla el Reglamento de Servicios Digitales para la publicidad en general, como las del Reglamento de Transparencia y Segmentación de la publicidad política. Estas disposiciones permitirán conocer quién está detrás de los mensajes pu-

blicitarios e incluso que técnicas de segmentación se han utilizado. También las disposiciones que ponen especial énfasis en el funcionamiento y técnicas utilizadas y sus efectos sobre el ejercicio de derechos fundamentales, en especial los que se encuentran relacionados con los procesos electorales. Así, pueden señalarse las disposiciones del Reglamento de Servicios Digitales que obligan a los prestadores de servicios de muy gran tamaño a evaluar los riesgos sistémicos que entraña el diseño, funcionamiento y uso de sus servicios, el uso indebido de estos, y la adopción de medidas para reducir dichos riesgos; o las disposiciones del Reglamento de transparencia y segmentación de la publicidad política, que detallan los requisitos a los que deben sujetarse las técnicas de segmentación y entrega de anuncios, y prohíben la utilización de técnicas de segmentación que impliquen la elaboración de perfiles que utilicen datos sensibles, como los de las opiniones políticas de las personas. Este tipo de disposiciones son sumamente importantes durante los procesos electorales, para tratar de prevenir que se usen los servicios de este tipo de plataformas, redes y motores de búsqueda para la realización de campañas de *microtargeting* electoral que pretendan alterar los resultados mediante la difusión de desinformación.

La combinación de las disposiciones de los distintos Reglamentos que se han examinado en el presente trabajo permitirá una mayor transparencia de todo tipo de publicidad en línea, incluida la política, un mayor control sobre los servicios digitales que se ofrecen en el mercado interior, y un abanico de medidas para luchar contra la desinformación y la difusión de contenidos ilícitos. Pero siguen existiendo limitaciones, especialmente al seguir basando en el consentimiento explícito la posibilidad del tratamiento de los datos. Las plataformas, a ese respecto, siguen gozando de una posición de privilegio en la que el usuario no está en posición de negociar. Aunque se requiere que se ofrezca una alternativa equivalente a los usuarios que rechacen la segmentación para recibir publicidad política, si el servicio resulta excesivamente limitado forzará al usuario a aceptar esa segmentación. Tampoco se restringe en exceso las posibilidades de segmentación, pues no se limita el número de categorías de datos que se pueden utilizar, lo que posibilita que pueda seguir realizándose una microsegmentación y que, aunque no se utilicen datos pertenecientes a las categorías especiales —como los de las opiniones políticas—, se pueden utilizar los intereses del usuario para enviar dicha publicidad pues de los mismos se infiere de forma indirecta la ideología.

Los sistemas de IA que se desarrollen, por su parte, también deberán sujetarse a una serie de requisitos establecidos por el nuevo Reglamento, quedando prohibidos los que supongan un riesgo inaceptable, reforzando la protección de los datos personales utilizados en el desarrollo de estos sistemas, y quedando los desarrolladores y proveedores sujetos a una serie de obligaciones. Como los demás Reglamentos, no solo busca mejorar el funcionamiento del mercado interior, sino que a través de sus disposiciones trata de proteger los derechos fundamentales y permitirá regular el uso de este tipo de sistemas en prácticas de *microtargeting* electoral. Ahora bien, también se enfrenta

a limitaciones pues, por ejemplo, las medidas de transparencia que propone pueden ser también fácilmente eludibles y la supervisión es difícil de llevar a cabo.

Puede decirse que se ha dado un paso para mejorar la situación anterior, pero siguen planteándose importantes retos. Las ingentes bases de datos disponibles y la utilización de herramientas de análisis predictivo han demostrado su gran potencial para influir en el comportamiento de los electores, por lo que aparte de garantizar la transparencia de la publicidad política, de reforzar las exigencias para el tratamiento de los datos de los usuarios, y para la aplicación de técnicas de segmentación, es cada vez más necesario una buena educación en el manejo de las redes sociales y desde una edad temprana. Los usuarios tenemos que ser más conscientes de los datos que compartimos, pero también cuando recibimos publicidad o determinadas noticias, ser capaces de comprobar si verdaderamente son ciertas o no. Al igual que desde niños se enseñan los peligros de Internet y las redes sociales, debería educarse en cómo contrastar información, la conveniencia de leer más de un medio de comunicación, contrastar las noticias, y no conformarse simplemente con leer un mero encabezado polémico. Debe recuperarse esta conciencia cívica, salir del individualismo y volver a fomentar espacios donde se pueda debatir y tener en cuenta las opiniones de los demás, buscando el interés común. La adopción de normas que tratan de combatir las técnicas de desinformación y manipulación que están poniendo en riesgo nuestras democracias por sí sola puede que no sea suficiente.

BIBLIOGRAFÍA

I. Libros y artículos

Álvarez Rodríguez, Ignacio. «Responsable y Encargado del Tratamiento». En VVAA, *Comentarios a la Nueva Ley de Protección de Datos*, 105-149. Madrid: Dilex, 2020.

Andrejevic, Mark y Zola Volcic. «From mass to automated media. Revisiting the 'filter bubble'». En Big *Data, Political Campaigning and the Law. Democracy and Privacy in the age of micro-targeting*, edited by Normann Witzledb, Moira Paterson and Janice Richardson, 17-33. New York: Routledge, 2020.

Arenas Ramiro, Mónica. «Partidos políticos, opiniones políticas e Internet: la lesión del derecho a la protección de datos personales». *Teoría y Realidad Constitucional*, núm. 44 (2019): 341-372, doi.org/10.5944/trc.44.2019.26005.

Arnaiz Chico, Elsa, «El colapso del ágora digital: como la IA generativa está enterrando la democracia». *El País*, marzo 2025. Acceso el 15 de marzo de 2025, www.elpais.es.

Ashraf, Anwar. «Las mentiras de Elon Musk sobre las elecciones en EE.UU.». *DW*, 2 de noviembre de 2024. Acceso el 7 de febrero de 2025, *https://www.dw.com/es/dw-verifica-c%C3%B3mo-elon-musk-est%C3%A1-difundiendo-mentiras-sobre-las-elecciones-estadounidenses/a-70685868*.

Bayo Pérez, Blanca. «Elecciones EE.UU. 2024. El uso de la IA como herramienta de desinformación en la campaña». *El País*, 3 de noviembre de 2024. Acceso el 10

de febrero de 2025, *https://www.rtve.es/noticias/20241103/elecciones-eeuu-2024-ia-herramienta-desinformacion-campana/16307898.shtml*

Blasi casagra, Cristina y Mathias Vermeulen. «Reflections on the murky legal practices of political micro-targeting from a GDPR perspective». *International Data Privacy Law*, Vol 11, No 4 (202): 348-359. doi.org/10.1093/idpl/ipab018.

Bruns, Axel. «El Filtro Burbuja». *Revista Latinoamericana de Economía y Sociedad Digital*, Nº especial 1 (julio, 2022). doi.org/10.53857/ndhq9707.

Díaz Crego, María. *Regulación de la publicidad política*. Servicio de Estudios del Parlamento Europeo, PE739.311, enero 2023.

European Commission for Democracy through Law (Venice Commission). *Joint Report of the Venice Commission and of the Directorate of Information Society and Action against crime of the Directorate General of Human Rights and Rule of Law (DGI) on Digital Technologies and Elections*, adopted by the Venice Commission at its 119th Plenary Session (Venice, 21-22 June 2019) CDL-AD (2019)016.

G. Gómez, Rosario. «La nueva ley de protección de datos alarma a los expertos». *El País*, 3 de diciembre de 2018. Acceso el 10 de febrero de 2025, *https://elpais.com/sociedad/2018/12/02/actualidad/1543765290_001106.html.*

García Mahamut, Rosario. «Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español». *Teoría y Realidad Constitucional* núm. 35 (2015): 309-338, doi.org/10.5944/trc.35.2015.14921.

García Sanz, Rosa María. «Tratamiento de datos personales de las opiniones políticas en el marco electoral: todo en interés público». *Revista de Estudios Políticos*, 183 (2019), 129-159, doi: *https://doi.org/10.18042/cepc/rep.183.05.*

Garrote de Marcos, María. «La IA en el período electoral: tres propuestas a partir de la integridad electoral». En *Fortalecimiento de la democracia y el Estado de Derecho a través de la inteligencia artificial*, ed. Por Rafael Bustos Gisbert, Javier García Roca, 259-281. Oñati: IVAP, 2025.

Giraldo Luque, Sergio y Cristina Fernández Rovira. «¿Radicalizan a los jóvenes las redes sociales?». *The Conversation*, 4 de marzo de 2025. Acceso el 5 de marzo de 2025. *https://theconversation.com/topics/jovenes-59211.*

González De La Garza, Luis Miguel. «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* nº 103 (septiembre-diciembre 2018): 257-302, doi.org/10.5944/rdp.103.2018.23203.

Hernández Peña, Juan Carlos. «Campañas electorales, Big Data y perfilado ideológico. Aproximación a su problemática desde el derecho fundamental a la protección de datos». *Revista Española de Derecho Constitucional*, 124 (2022): 41-73. Doi: *http$3doi.org/10.18042/cepc/redc.124.02.*

Hernández Ramos, Mario. «La Convención Marcos del Consejo de Europa sobre inteligencia artificial y derechos humanos, democracia y Estado de Derecho. El primer tratado internacional en la materia». En *Fortalecimiento de la democracia y el Estado de Derecho a través de la inteligencia artificial*, ed. por Rafael Bustos Gisbert, Javier García Roca, 93-187. Oñati: IVAP, 2025.

Horwitz, Jeff. *Broken Code. Inside Facebook and the fight to expose its harmful secrets.* New York: Doubleway, 2023.

Huber, Ludwig. *Democracia 2.0: El poder político en la era digital*. Perú: IEP, 2023.

Daniel Iriarte. «Todo lo que Elon Musk está haciendo para que Trump gane las elecciones». *El Confidencial*, 24 de octubre de 2024. Acceso el 11 de febrero de 2025, *https://www.elconfidencial.com/mundo/2024-10-24/elon-musk-campana-trump-elecciones-eeuu_3989361/*

López Calera, Nicolás. «El interés público: entre la ideología y el Derecho». *Anales de la Cátedra Francisco Suárez* nº 44 (2010): 123-148. doi: *https://doi.org/10.30827/acfs.v44i0.502*.

Mars, Amanda. «Trump acusa sin pruebas a Biden de querer "robar" las elecciones con "votos ilegales"». *El País*, 6 de noviembre de 2020. Acceso el 10 de febrero de 2025, *https://elpais.com/internacional/elecciones-usa/2020-11-06/trump-acusa-sin-pruebas-a-biden-de-querer-robar-las-elecciones-con-votos-ilegales.html*

McDonagh, Maeve. «Freedom of processing of personal data for the purpose of electoral activities after the DGPR». En *Big Data, Political Campaigning and the Law. Democracy and Privacy in the age of micro-targeting*. Edited by Normann Witzledb, Moira Paterson and Janice Richardson, 114-138. New York: Routledge, 2020.

Merlo, Carlos. *Data Science Electoral.* México: Anderson Publishing, 2021.

Modrón Lecue, Irene. «¿Qué es el código abierto en el que se basa la IA DeepSeek y cómo contribuye al desarrollo de la tecnología?». *RTVE*, 10 de febrero de 2025. Acceso el 15 de marzo de 2025, www.elpais.es

Ortiz, Rubén. «Cómo hacer *microtargeting* con publicidad digital». *SEOCOM*, 4 de diciembre de 2024. Acceso el 17 de febrero de 2025, *https://seocom.agency/blog/como-hacer-microtargeting-con-nuestra-publicidad/*.

Pérez-Escolar, Marta y Purificación Alcaide-Pulido, «La polarización ideológica y la desinformación como estrategias propagandísticas en la guerra híbrida» en *Desinformación y Defensa. Conflictos híbridos, entorno cognitivo y operaciones de influencia*, Juan Miguel Aguado y otros, 71-92. Madrid: Dykinson, 2024.

Piore, Adam. «Technologists are trying to fix the "filter bubble" problem that tech helped create». *MIT Technology Review,* 30/8/2018. Acceso el 20 de febrero de 2025, *https://www.technologyreview.com/2018/08/22/2167/technologists-are-trying-to-fix-the-filter-bubble-problem-that-tech-helped-create/*

Polo Roca, Andoni. «Protección de datos y elaboración de perfiles: el nuevo artículo 58 bis de la Ley orgánica 5/1985, de 19 de junio, del régimen electoral general». *Revista Galega de Administración Pública (REGAP)* núm. 58 (julio-diciembre 2019): 507-527. doi: 10.36402/regap.v1i58.46.

Praiser, Eli. *El filtro burbuja. Cómo la red decide lo que leemos y lo que pensamos*. Taurus, 2017.

Richardson, Janice; Norman Witzleb y Moira Paterson. «Political micro-targeting in an era of big data analytics. An overview of the regulatory issue». En *Big Data, Political Campaigning and the Law. Democracy and Privacy in the age of micro-targeting*. Edited by Normann Witzledb, Moira Paterson and Janice Richardson, 1-14. New York: Routledge, 2020.

Richardson, Janice. «Filter bubbles, democracy and conceptions of self. A brief genealogy and a Spinozist perspective». En Big *Data, Political Campaigning and the Law. Democracy and Privacy in the age of micro-targeting*, edited by Normann Witzledb, Moira Paterson and Janice Richardson, 34-46. New York: Routledge, 2020.

Rodríguez Fernández, Leticia. *Propaganda digital. Comunicación en tiempos de desinformación*. Barcelona: Editorial UOC, 2021.

Rodríguez-Izquierdo, Miryam. «El mercado interior y la manipulación informativa con finalidad electoral». Comunicación presentada al XXI Congreso de la ACOES: Constitución y Elecciones, Valladolid, 27 y 28 de marzo de 2024.

Rubio Núñez, Rafael. «La amenaza tecnológica en los procesos electorales: una respuesta jurídica». *Revista de privacidad y derecho digital*, vol. 3, Núm. 11 (julio-septiembre 2018):109-146.

Saura García, Carlos. «Microtargeting político y vigilancia social masiva: impactos negativos en las democracias occidentales». *Daimon. Revista Internacional de Filosofía*, nº 93 (Septiembre-Diciembre 2024): 73-89. doi.org/10.6018/daimon.609851.

Silva C., Sebastián. «Donald Trump y Elon Musk: la desinformación al poder». *Sinc*, 5 de febrero de 2025. Acceso el 7 de febrero de 2025, *https://www.agenciasinc.es/Opinion/Donald-Trump-y-Elon-Musk-la-desinformacion-al-poder*

Sarah Steffen. «Fact check: Disinformation's impact on the US election». *DW*, 11 de julio de 2024. Acceso el 11 de febrero de 2025, *https://www.dw.com/en/fact-check-what-role-did-disinformation-play-in-the-us-election/a-70729575*.

Steiger, Dominik. «International law and new challenges to democracy in the digital age. Big data, privacy and interverences with the political process». En Big *Data, Political Campaigning and the Law. Democracy and Privacy in the age of micro-targeting*, edited by Normann Witzledb, Moira Paterson and Janice Richardson, 71-98, New York: Routledge, 2020.

Tusset Varela, Damián. «Cuando la IA decide: fronteras legales y éticas de la IA en el sistema electoral». *Diario La Ley*, 30/1/2024. Acceso el 12 de enero de 2025, *https://diariolaley.laleynext.es/dll/2024/02/02/cuando-la-ia-decide-fronteras-legales-y-eticas-de-la-ia-en-el-sistema-electoral*.

Vosoughi, Soroush; Deb Roy y Sinan Aral. «The Spread of true and false news online», *Science* vol. 359, issue 6380 (2018):1146-1151. DOI: 10.1126/science.aap9559.

II. Normativa

Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DOUE nº 119, de 4 de mayo de 2016.

Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política. DOUE nº 900, de 20 de marzo de 2024.

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. DOUE nº 1689, de 12 de junio de 2024.

Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales. DOUE nº 277, de 27 de octubre de 2022.

Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital. DOUE nº 265, de 12 de octubre de 2022.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE nº 294, de 6 de junio de 2018.

III. Jurisprudencia

TEDH

Observer y Guardian c. Reino Unido, 26 de noviembre de 1991.

Rekvényi c. Hungría, 20 de mayo de 1999.

Hashman y Harrup c. Reino Unido, 25 de noviembre de 1999.

Maestri c. Italia, 17 de febrero de 2004.

TJUE

Digital Righst Ireland Ltd, asuntos acumulados C-293/12 y C-594/12.
Google España c. AEPD y Mario Costeja González, asunto C-131/12.
Schrems I, asunto C-362/14.
Schrems II, asunto C-311/18.
Eva Glawischnig-Piesczek contra Facebook Ireland Limited, asunto C-18/18.
La Quadrature du Net vs. France, asuntos acumulados C-511/18, C-512/18 y C-520/18.
OQ y Land Hessen, asunto C-634/21.

TC

STC 20/1990, de 15 de febrero.
STC 254/1993, de 20 de julio.
STC 143/1994, de 9 de mayo.
STC 119/1995, de 17 de julio.
STC 76/2019, de 22 de mayo.
STC 292/2000, de 30 de noviembre.

IV. Otros documentos

AEPD. *Criterio de la Agencia Española de Protección de Datos sobre cuestiones electorales en el proyecto de nueva LOPD*, 21 de noviembre de 2018.

CCPR. General Comment No. 25: Article 25 (Participation in Public Affairs and the Right to Vote), The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service.

Comisión Europea. «Código de buenas prácticas en materia de desinformación de 2022». Acceso el 10 de marzo de 2025, *https://digital-strategy.ec.europa.eu/es/policies/code-practice-disinformation*

Comité Europeo De Protección De Datos. Declaración 2/2019 sobre el uso de datos personales durante las campañas políticas, de 13 de marzo de 2019.

Consejo De La Unión Europea. «La UE introduce nuevas normas sobre transparencia y segmentación en la publicidad política», 11/3/2024. Acceso el 10 de marzo de 2025. *https://www.consilium.europa.eu/es/press/press-releases/2024/03/11/eu-introduces-new-rules-on-transparency-and-targeting-of-political-advertising/*

Consejo Europeo/Consejo De La Unión Europea. *Reglamento de Mercados Digitales*, acceso el 13 de marzo de 2025, *https://www.consilium.europa.eu/es/policies/digital-markets-act/*

Council of Europe. *Internet and electoral campaigns. Study on the use of Internet in electoral campaigns*. DGI (2017)11.

Edri. «Proceed with caution: Flexibilities in the General Data Protection Regulation», 5 July 2016.

EUR-lex. «Reglamento de Servicios Digitales». Acceso el 13 de marzo de 2025, *https://eur-lex.europa.eu/ES/legal-content/summary/digital-services-act.html*

Grupo De Trabajo Sobre Protección De Datos Del Artículo 29. «Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679», adoptadas el 3 de octubre de 2017, SP251rev.01.

Grupo de Trabajo sobre Protección de Datos del artículo 29. «Dictamen 6/2014», de 9 de abril de 2014.

Maldita.es. «"Kamala Harris proisraelí" si eres musulmán y "propalestina" si eres judío: así acaban donaciones de Elon Musk en anuncios contra la candidata demócrata», 21/10/2024. Acceso el 7 de febrero de 2025, *https://maldita.es/malditatecnologia/20241021/anuncios-musk-contra-kamala-harris/*

Meta. «Segmentación de anuncios. Consigue que tus anuncios lleguen a personas a las que les encantará tu empresa». Acceso el 16 de diciembre de 2022. *https://es-es.facebook.com/business/ads/ad-targeting*.

Meta. «¿Cómo usar audiencias personalizadas o similares?». Acceso el 14 de marzo de 2023. *https://es-es.facebook.com/business/help/572787736078838?id=176276233019487*.

Meta. «Píxel de Meta». Acceso el 16 de diciembre de 2022. *https://es-es.facebook.com/business/tools/meta-pixel*

Supervisor Europeo de Protección de Datos. *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, 11 April 2017.