

Algoritmos, Inteligencia Artificial y procesos electorales: riesgos para el pluralismo político y la integridad democrática

Amalia LOZANO ESPAÑA*

Sumario. 1. Introducción 2. Desafíos sistémicos para las elecciones y el pluralismo electoral 3. La respuesta normativa europea frente a los riesgos democráticos de las plataformas digitales y la inteligencia artificial 4. El etiquetado obligatorio y sanciones por contenido IA no identificado en España e Italia 5. Conclusiones

1. Introducción

Las plataformas digitales y los motores de búsqueda se han transformado en espacios centrales para el debate público, configurando tanto la opinión pública como el comportamiento electoral. Estas tecnologías funcionan a través de algoritmos que operan como nuevos centros de poder, provocando la “destrucción de la política y el debilitamiento de los valores y los derechos constitucionales”¹. Sin embargo, estas no actúan de manera autónoma; detrás de ellas intervienen mayoritariamente grandes multinacionales con el objetivo de obtener beneficios económicos².

La aparición de las redes sociales ha representado una nueva tensión sobre los valores que propugna el constitucionalismo – aunque anteriormente ya habían empezado a entrar en disputa no solo interna, sino también externamente³ – pues estas suponen un “escaparate de las alternativas en materia de valores al tiempo que desarrollan y apuestan por sus propios valores”⁴. Como ya alertaba Castells (2008), “la emergencia de la autocomunicación de masa desintermedia a los medios y abre el abanico de influencias en el campo de la comunicación”⁵. En un contexto donde se mejora constantemente el envío y distribución de nueva información⁶, gracias a los sistemas algorítmicos se

* Contratada predoctoral por la Universidad de Granada en el Departamento de Derecho Constitucional y en cotutela con la Università di Bologna.

¹ Cfr. F. Balaguer Callejón, *La Constitución del Algoritmo. El difícil encaje de la Constitución analógica en el mundo digital*, en F. Balaguer Callejón y L. Cotino Hueso (coords.), *Derecho público de la inteligencia artificial*. Zaragoza (Fundación Manuel Jiménez Abad), 2022, p. 52.

² *Ibid.*, p. 52.

³ Por un lado, externamente la globalización, las empresas multinacionales y los organismos supranacionales comenzaron a limitar la soberanía estatal, sobre este tema véase: J. Habermas *La constelación posnacional*, 1998; L. Ferrajoli, *Poderes salvajes: la crisis de la democracia constitucional*, Madrid, 2011, mientras que la creciente judicialización de la política cuestionaba el equilibrio entre tribunales y parlamentos (cfr. B. Ackerman, *We the People, volumen I: Foundations*, Harvard, 1991; R. Hirschl, *Towards Juristocracy*, Harvard, 2004). A esto se sumó el auge del populismo, que en nombre de la voluntad popular socavaba las estructuras liberales (véase S. Levitsky y D. Ziblatt, *How Democracies Die*, Nueva York, 2018), y la incapacidad de las constituciones para garantizar efectivamente los derechos sociales frente a la desigualdad (cfr. T. Piketty, *El capital en el siglo XXI*, París, 2013).

⁴ A. Calahorra Aguilar, *Valores constitucionales y sociedad digital*, en *Revista da AJURIS-Qualis A2*, 49(152) /2022, p. 354.

⁵ M. Castells, *Comunicación, poder y contrapoder en la sociedad red (I). Los medios y la política*, en *Telos: Cuadernos de comunicación e innovación*, 74/2008, p. 13.

⁶ *Ibid.*

consigue “maximizar el tiempo que los usuarios pasan en las plataformas para poder así extraer datos y posteriormente comercializarlos con fines publicitarios”⁷.

La intensa regulación del procedimiento electoral, especialmente en lo relativo a la campaña, respondía a una lógica de control previo. En la actualidad, las amenazas que originalmente se buscaban prevenir han quedado superadas o ya no constituyen los principales riesgos. Sin embargo, el debate se está suscitando en la influencia de las redes, incluyendo aspectos como la campaña, la propaganda política⁸, y el uso de tecnologías y algoritmos que pueden incidir en la formación de la voluntad popular. De hecho, el Tribunal Europeo de Derechos Humanos en el asunto *Bradshaw y otros contra Reino Unido*⁹ ha dictaminado que, aunque puedan difundir información directamente al electorado, también han hecho posible que actores hostiles propaguen desinformación a una escala y con una rapidez nunca vistas, suponiendo una amenaza significativa para la democracia. Por otra parte, comienza a postularse que el derecho constitucional se centre no solo en la perspectiva de los derechos, sino también en los deberes tal como plantea Zagrebelsky¹⁰.

La Inteligencia Artificial se ha insertado en esta compleja realidad y está alterando aún más el normal desarrollo de estos procedimientos, e incluso emergiendo como “potencial instrumento de toma de decisiones políticas y jurídicas”¹¹, interfiriendo en la “cadena de legitimidad en la que sus eslabones conecten con el principio democrático”¹². En este sentido, señala Rubio Núñez cómo la propaganda enviada a través de Inteligencia Artificial (en adelante IA) ha permitido mejorar la capacidad de envío de mensajes personalizados en redes, lo que ha provocado que se fragmente aún más el debate público¹³ y que el discurso político se centre mayoritariamente en aspectos más irracionales y sentimentales de las personas¹⁴. La publicidad política está suponiendo un grave riesgo ya que esta se inserta en la actualidad dentro de mensajes sin aparente contenido político mediante técnicas como el *scrolling*. Estos procesos constituyen el núcleo de funcionamiento de las nuevas plataformas como *TikTok*, las cuales están redefiniendo la sociedad no solo culturalmente, sino también política y jurídicamente¹⁵. Pero no se puede olvidar que estas plataformas, en gran parte, operan sobre datos¹⁶. Desde un punto de vista jurídico, el problema principal radica en que el uso de algoritmos y de nuevos sistemas de inteligencia artificial a partir de los datos que extraen del uso de estas plataformas, hacen que sean cada vez más predictivos permitiendo a través de las plataformas el envío de publicidad más personalizada. En el caso de los procesos electorales, esta lógica ha alimentado la información positiva que recibían sobre determinados candidatos y los mensajes negativos en contra de otros candidatos.

Los nuevos riesgos en las campañas electorales y la integridad de estos procesos se han señalado por parte de la Comisión Europea en las *Directrices para los proveedores de Plataformas en Línea de*

⁷ A. Barredo Artiguez, *El Reglamento Europeo de Servicios Digitales y la defensa de la democracia*, en *Revista de Derecho Político*, 122/2025, pp. 295–326.

⁸ L. Pegoraro, *¿Guardianes de las elecciones o garantes de la democracia?*, en L. Pegoraro, G. Pavani (coords.), *El guardián de las elecciones. El control electoral en perspectiva comparada*, Bogotá, Tirant lo Blanch, 2015.

⁹ Tribunal Europeo de Derechos Humanos (Sección Cuarta), *Caso Bradshaw y otros c. Reino Unido*, núm. 15653/22, 22 de julio de 2025.

¹⁰ G. Zagrebelsky, *Derechos a la fuerza*, Madrid, 2023.

¹¹ Cfr. J.F. Sánchez Barrilao, *El Impacto de la Inteligencia Artificial en los procesos democráticos*, en *Revista de Derecho Constitucional Europeo*, 43/2025.

¹² Id., *Inteligencia artificial y fuentes del derecho*, en *Revista de Derecho Constitucional Europeo*, 39/2023.

¹³ Cfr. R. Rubio Núñez, *El uso de la inteligencia artificial en las campañas electorales y sus efectos democráticos*, en *Revista de Derecho Político*, 122/2025, p. 65 ss.

¹⁴ *Ibid.*

¹⁵ Véase sobre la influencia del algoritmo en el derecho constitucional: F. Balaguer Callejón (2022). *La Constitución del algoritmo*, Zaragoza (Fundación Giménez Abad).

¹⁶ S. Finn, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, en *Analisi Giuridica dell'Economia*, 18(1)/2019, pp. 110-111.

*Muy Gran Tamaño y Motores de Búsqueda en Línea de Muy Gran Tamaño*¹⁷. Estos se especifican a continuación, sin obviar que la Comisión ha indicado que no es una lista cerrada: “la proliferación de discursos de odio ilegales en Internet, las amenazas vinculadas a la manipulación y a la injerencia informativa extranjera (“FIMI”), así como el fenómeno más amplio de la desinformación, la difusión de contenidos extremistas (violentos) y aquellos orientados a la radicalización de las personas, junto con la propagación de materiales generados mediante nuevas tecnologías, como la inteligencia artificial generativa”¹⁸. Las elecciones en Rumanía han sido un ejemplo de los nuevos riesgos sistémicos para la integridad de los procesos electorales y el pluralismo político. Anteriormente, el caso *Cambridge Analytica* mostró ya las posibilidades de manipulación encubierta del comportamiento electoral mediante técnicas de microsegmentación, psicografía y generación de contenidos sin trazabilidad.

Ante los riesgos que plantea el uso de la publicidad y el envío de mensajes personalizados durante las campañas electorales, se han diseñado marcos normativos a nivel europeo¹⁹, a la par que los Estados miembros están reaccionando con sus propias regulaciones²⁰, surgiendo mecanismos de moderación e intervención que aseguren el interés general para garantizar el pluralismo político y la democracia²¹. Es este contexto donde se encuadra el presente trabajo. En él se profundiza, a partir de estas manifestaciones que han tenido un impacto en el núcleo de nuestras democracias, en la nueva regulación destinada a delimitar esa dimensión pública que han adquirido las plataformas.

El artículo trata de analizar cómo la irrupción de las plataformas digitales, los motores de búsqueda y, especialmente, los sistemas de IA aplicados a la publicidad política personalizada han transformado el espacio público de debate, generando nuevos riesgos para la integridad electoral y el pluralismo político. Examina el papel de los algoritmos en la creación de *filter bubbles*, *echo chambers* y flujos informativos hipersegmentados que pueden condicionar el comportamiento electoral, los cuales se han amplificado con nuevas plataformas como *TikTok*, así como las implicaciones constitucionales y jurídicas de estas prácticas: en particular, en cómo está afectando a los procesos electorales. Se ha elegido su análisis desde dos ámbitos, el nacional y el europeo, ya que en la actualidad la problemática que plantean estos mecanismos supera los confines del Estado-nación, afectando a los procesos democráticos en diferentes niveles nacionales, regionales y supranacionales. De este modo se examinará el marco normativo europeo – incluidos el Reglamento de Servicios Digitales, el Reglamento de Inteligencia Artificial y la futura Ley española de IA²² –, destacando sus mecanismos de supervisión, transparencia y sanción, y señalando los desafíos que persisten en la protección de derechos fundamentales y en la coordinación entre autoridades competentes. En este sentido, se utilizarán referencias a la reciente aplicación de la normativa europea en Rumanía. En cuanto al ámbito nacional se profundizará en la propuesta de regulación de la inteligencia artificial con algunas referencias de derecho comparado a la nueva legislación italiana sobre esta cuestión.

¹⁷ Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes, (<https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes>).

¹⁸ *Ibid*, apartado primero.

¹⁹ Véase: Reglamento General de Protección de Datos (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. El Reglamento (UE) 2022/2065 conocido la Ley de Servicios Digitales. Reglamento (UE) 2022/1925 conocido como la Ley de Mercados Digitales (DMA). Especialmente, el Reglamento (UE) 2024/900 sobre transparencia y segmentación de la publicidad política adoptado en marzo de 2024, entrada en vigor a partir de otoño de 2025. Hay que mencionar, también, el Plan de Acción para la Democracia Europea, COM (2020) 790 final.

²⁰ Ejemplos, en Francia, la *Loi n° 2018-1202 relative à la manipulation de l'information*. En Alemania, la ley conocida como *Netzwerkdurchsetzungsgesetz (NetzDG)* (2017).

²¹ V.J. Vázquez Alonso, *La obsolescencia probable*, cit.

²² Reglamento (UE) 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). Ley de Inteligencia Artificial, regulada en el Reglamento (UE) 2024/1689, versión del Diario Oficial de 13 de junio de 2024. También, el anteproyecto de ley para el buen uso y la gobernanza de la Inteligencia Artificial, actualmente en fase de consulta pública (<https://avance.digital.gob.es/es-es/Participacion/Paginas/DetalleParticipacionPublica.aspx?k=468>).

2. Desafíos sistémicos para las elecciones y el pluralismo electoral

Los nuevos riesgos en las elecciones son un ejemplo más de cómo la globalización y la digitalización han provocado dos consecuencias en el constitucionalismo sobre los derechos: por un lado, se ha pasado a un escenario global a través de las redes sociales y de flujos de comunicación; y, por otro lado, se han trasladado desde la esfera pública a una privada²³. Una de las consecuencias directas de esta nueva realidad digital afecta al pluralismo político, uno de los principios esenciales de nuestros sistemas democráticos; como advierte García Sanz (2019), puede verse distorsionado por “una manipulación de los datos en la Red”²⁴.

Este estudio parte de una perspectiva interdisciplinaria, entendiendo que el Derecho, y en particular el constitucional comparado, debe incorporar los aportes de la Ciencia Política y la Psicología²⁵, especialmente en el análisis de fenómenos contemporáneos como la propaganda política desarrollada a través de las redes sociales y los sistemas de inteligencia artificial.

Los fenómenos de desinformación constituyen un catalizador de la polarización, reduciendo el pluralismo informativo y, en consecuencia, disminuyendo la calidad democrática²⁶. La desinformación incluye noticias falsas (*fake news*) – contenidos inventados con intención de engañar²⁷ –, *misinformation* – información engañosa, es decir, datos incorrectos difundidos a diferencia de las *fake news* sin intención deliberada²⁸ –, las *deepfakes* – uso de IA para generar imágenes, audios o vídeos falsos que simulan declaraciones o conductas de figuras políticas²⁹ – y microsegmentación opaca – mensajes dirigidos a grupos muy específicos basados en perfiles psicológicos o ideológicos –.

El caso *Cambridge Analytica* evidenció ya los riesgos de manipulación de los datos con consecuencias en el funcionamiento de los procesos democráticos de varios países³⁰. En este caso, se situó en el centro de la cuestión, pues se pusieron de manifiesto nuevos riesgos para las democracias. Primero, la emergencia de las campañas *data-driven*, es decir, se pasa de campañas de persuasión masiva a unas campañas basadas en análisis de datos para identificar “quién es persuadible”³¹ y enviarle mensajes específicos; segundo, la cuestión de la personalización del contenido político mediante la utilización de las técnicas de la psicografía en los votantes – una aproximación psicológica de la personalidad mediante la utilización de encuestas online³² –; y tercero, *el clustering* – mediante la combinación de técnicas algorítmicas y la huella digital que dejan los usuarios en redes sociales³³ –. De esta forma se consiguió el perfilado ideológico de miles de votantes³⁴.

²³ F. Balaguer Callejón, *Data protection and the transformation of rights in the digital society*, en *UNIO – EU Law Journal*, 10(1)/2024, p. 3 ss.

²⁴ R.M. García Sanz, *Tratamiento de Datos Personales de las opiniones políticas en el marco electoral: todo en interés público*, en *Revista de Estudios Políticos*, 183/2019, p. 129 ss.

²⁵ L. Pegoraro, *El método comparativo*, en L. Pegoraro, *Sistemas constitucionales comparados*, 2025, p. 26.

²⁶ J.A. Tucker, A. Guess, P. Barbera, C. Vaccari, A. Siegel, S. Sanovich, D. Stukal, B. Nyhan, *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, Hewlett Foundation Report, 2018.

²⁷ Véase: S. Vosoughi, D. Roy, S. Aral, *The spread of true and false news online*, en *Science*, 359(6380) /2018, pp. 1146-1151. En línea opuesta, H. Allcott, M. Gentzkow, *Social media and fake news in the 2016 election*, en *Journal of Economic Perspectives*, 31(2) /2017, p. 211 ss. Estos autores han demostrado que las redes sociales no aceleraron de forma sustancial la polarización ideológica en Estados Unidos y que el impacto de las *fake news* en las elecciones fue, en términos de voto, marginal.

²⁸ C. Wardle, H. Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe Report, 2017.

²⁹ D. Fallis, *The Epistemic Threat of Deepfakes*, en *Philosophy & Technology*, 34(1) /2021, p. 623 ss.

³⁰ Véase: C.J. Bennett, D. Lyon, *Data-driven elections: Implications and challenges for democratic societies*, en *Internet Policy Review*, 8(4)/2019.

³¹ E. Hersh, *Hacking the Electorate: How Campaigns Perceive Voters*, Cambridge, 2015.

³² Caso Cambridge Analytica mediante la utilización de encuestas como el *Test Ocean*.

³³ Cfr. J.C. Hernández Peña, *Campañas electorales, big data y perfilado ideológico. Aproximación a su problemática desde el derecho fundamental a la protección de datos*, en *Revista española de derecho constitucional*, 124/2022, pp. 48-49.

³⁴ Se ha señalado que 50 millones de usuarios de Facebook mediante una app denominada *This Is Your Digital Life*, creada por el académico Aleksandr Kogan. Aunque solo unas 270 000 personas participaron directamente, se obtuvieron datos de sus contactos gracias a la API de Facebook. De esos 50 millones, aproximadamente 30 millones fueron usados para crear perfiles

En primer lugar, estos procesos se amplifican mediante el uso de *bots* o el envío de mensajes automatizados, y se combinan con las llamadas *echo chambers* y las *filter bubbles*. Las *echo chambers* se caracterizan por reforzar y magnificar los mensajes dentro de un espacio cerrado, aislándolos de cualquier refutación³⁵. Por su parte, las *filter bubbles* surgen de la personalización algorítmica: las plataformas digitales, a través de decisiones automatizadas sobre la presentación de contenidos, crean un espacio personal para cada usuario de contenido que recibe³⁶; el usuario no elige la información, sino que recibe aquella adaptada a su comportamiento en línea³⁷. Las consecuencias de estos fenómenos son que reducen la diversidad de contenidos y que los usuarios reciben información afín a sus intereses afectando, en concreto, a la capacidad de distribución y a la demanda de comunicación en un entorno caracterizado por una amplia oferta de medios³⁸. En el contexto de estos mensajes políticos personalizados, resulta más complicado detectar la desinformación, debido a que el número de mensajes recibidos y noticias enviadas veraces se entremezcla con los debates políticos diseñados con la intención de desinformar³⁹.

En segundo lugar, para entender el perfilado ideológico, debe partirse de cómo la propaganda política, entendida como aquel contenido que incluye “mensajes con relevancia electoral”⁴⁰, se ha transformado en el entorno mediático digital. En un ecosistema donde el público puede elegir entre gran variedad de contenidos, la publicidad política ha demostrado ser, en muchos casos, el único contacto con la información política de muchos ciudadanos poco motivados. De este modo, los *spots* políticos tienen más alcance que las noticias tradicionales⁴¹. La problemática de esta propaganda política personalizada surge de la utilización de algoritmos con *big data* que permiten perfilar psicoideológicamente a los ciudadanos. El pluralismo se ve afectado porque la competencia entre partidos ya no se da en torno a programas políticos abiertos, sino en la explotación de las debilidades

psicográficos en base al modelo de personalidad *Big Five* (OCEAN), combinándolos con otros registros para segmentar votantes con alta precisión (<https://www.bbc.com/mundo/noticias-49093124>).

³⁵ Cfr. K.H. Jamieson, J.N. Cappella, *Echo chamber: Rush Limbaugh and the conservative media establishment*, Oxford-Nueva York, 2008, p. 76. Lo definieron como “un espacio mediático delimitado y cerrado que tiene el potencial de magnificar los mensajes transmitidos en su interior y aislarlos de cualquier refutación” (p. 76).

³⁶ Cfr. E. Pariser, *The filter bubble: How the new personalized web is changing what we read and how we think*, Penguin, Londres, 2011, p. 10. Las *filter bubbles* aluden, como señala la autora, a la personalización algorítmica de los contenidos, que genera “un universo único de información para cada uno de nosotros” (p. 10). Esto reduce la diversidad informativa y ofrece al usuario noticias más afines.

³⁷ A. Ross Arguedas, C. Robertson, R. Fletcher, R. Nielsen, *Echo chambers, filter bubbles, and polarisation: a literature review*, Reuters Institute for the Study of Journalism, 2022, p. 11.

³⁸ La discusión sobre estos fenómenos está abierta en cuanto a su papel en las elecciones: así parece demostrarse en el papel determinante de la autoselección; es decir, las personas siguen eligiendo contenidos en función de sus intereses y afiliaciones, lo que incrementa la polarización afectiva, más vinculada a emociones y actitudes hacia los otros que a una polarización ideológica estricta, véase: A. Bruns, *Are Filter Bubbles Real?*, Cambridge, 2019, planteó ha argumentado que esta visión es exagerada, ya que la mayoría de los usuarios sigue expuesta a contenidos variados y que la polarización responde más a dinámicas de auto-selección que a una selección algorítmica. Frente a estas posiciones más escépticas, S. Messing, S.J. Westwood, *Selective exposure in the age of social media: Endorsements trump partisan source affiliation when selecting news online*, en *Communication Research*, 41(8)/2014, p. 1042 ss., evidenciaron que los algoritmos de recomendación condicionan la percepción política de los votantes, moldeando tanto sus actitudes como su exposición a la información. De manera complementaria, D. Massand, N. Nath, *Filter bubbles and the Brexit surprise effect*, en *arXiv*, 2018, explican cómo estas burbujas informativas contribuyen al llamado “factor sorpresa” en procesos como el Brexit, al generar una percepción distorsionada de la opinión pública. En conjunto, la literatura muestra una tensión entre quienes consideran las *filter bubbles* un elemento central en la transformación de las elecciones y quienes relativizan su impacto directo sobre el voto, aunque existe consenso en que sí influyen en la calidad del debate público y en el pluralismo democrático. Junto con otros que hablan de una polarización afectiva, cfr. K. O'Hara, D. Stevens, *Echo chambers and online radicalism: Assessing the Internet's complicity in violent extremism*, en *Policy & Internet*, 7(4)/2015, pp. 401-422.

³⁹ M. Brkan, *The regulation of data-driven political campaigns in the EU: from data protection to specialized regulation*, en *Yearbook of European Law*, 41/2022, p. 348 ss.

⁴⁰ O. Muñoz Sánchez, *La regulación de las campañas electorales en la era digital: desinformación y microsegmentación en las redes sociales con fines electorales*, Madrid (Centro de Estudios Políticos y Constitucionales), 2020.

⁴¹ M. Prior, *News vs. entertainment: How increasing media choice widens gaps in political knowledge and turnout*, en *American Journal of Political Science*, 49(3)/2005, p. 577 ss.

individuales de los votantes⁴². El pluralismo político debe entenderse no solamente desde la óptica individual de elección, manifestación de diversas posiciones ideológicas y concurrencia de distintos grupos, sino también en la capacidad de acceso de los diversos grupos sociales al proceso político y a difundir su programa electoral de manera libre, no solamente entre sus propios votantes estrechamente unido a la libertad política como elemento de esta⁴³.

La tercera cuestión, una vez analizados el perfilado ideológico y la desinformación, es la microsegmentación de mensajes políticos sobre temas sensibles⁴⁴. Frente a la concepción clásica de una opinión pública que se forma mediante el contraste abierto de diferentes puntos de vista – incluso erróneos –, asistimos hoy a la configuración de un espacio múltiple y fragmentado⁴⁵, en el que resulta cada vez más difícil articular consensos generales. La microsegmentación opera mediante el envío de mensajes dirigidos, elaborados tras el perfilado previo de los votantes, con el fin de identificar temas de conflicto y diferenciarlos entre grupos específicos de votantes. Este mecanismo conduce a que el debate público quede artificialmente reducido a dichos asuntos, lo que implica una limitación del “mercado de las ideas”⁴⁶, pilar fundamental en una sociedad democrática y pluralista.

Estos tres procesos no deben confundirse; por un lado, se encuentran el perfilado ideológico, por otro, las campañas de desinformación y, diferente a estos dos, se encuentra la microsegmentación. Así, se debilita el pluralismo político, se incrementa la polarización y se transforma la condición misma del ciudadano: el sujeto constitucional, titular de derechos y libertades, pasa a ser reconvertido en un usuario consumidor⁴⁷, e incluso en un objeto mercantilizado, al explotarse y comercializarse sus datos personales como insumo central de la propaganda electoral⁴⁸.

Estas técnicas se han perfeccionado con la incorporación de la IA predictiva, que permite la introducción del *scrolling* en las plataformas digitales⁴⁹ a través del rastreo de sus preferencias. A diferencia de los algoritmos probabilísticos, la IA se basa en algoritmos predictivos – especialmente el *machine learning* y el *deep learning* – que aprenden de los datos para identificar patrones y tomar decisiones reproduciendo así una capacidad propia de la inteligencia humana⁵⁰. Dichas herramientas influyen directamente en la publicidad electoral difundida en redes sociales, dentro de campañas que combinan usuarios voluntarios o pagados con el uso de *bots* automatizados para amplificar mensajes. El fenómeno del *scrolling*, al interactuar con los algoritmos de recomendación, permite que determinados contenidos se posicionen con mayor frecuencia en los *feeds* de grupos concretos, reforzando la exposición selectiva. Esta dinámica incrementa la polarización, dado que los individuos filtran y eligen aquellos contenidos que confirman sus propias creencias, lo que a su vez intensifica los sesgos cognitivos en la forma en que interpretan y recuerdan la información política⁵¹. En estos casos, se utilizan los algoritmos predictivos que actúan a través de los propios histo-

⁴² M. Brkan, *The regulation of data-driven political campaigns in the EU*, cit., pp. 348-373.

⁴³ M. Sánchez Azpitarte, *Constitución del pluralismo y método jurídico*, en *Teoría y Realidad Constitucional*, 21/2008, pp. 451-452.

⁴⁴ J.C. Hernández Peña, *Campañas electorales, big data y perfilado ideológico*, cit., p. 50.

⁴⁵ R.M. García Sanz, *Tratamiento de Datos Personales de las opiniones políticas en el marco electoral: todo en interés público*, en *Revista de Estudios Políticos*, 183/2019, p. 129 ss.

⁴⁶ Oliver Wendell Holmes Jr., “dissenting opinion”, en *Abrams v. United States*, 250 U.S. 616 (1919), donde el juez introdujo la metáfora del mercado de las ideas al sostener que la libertad de expresión constituye el mejor medio para que la verdad prevalezca en la libre competencia de las opiniones.

⁴⁷ A. Aguilar Calahorra, *El sujeto de derecho en la sociedad del consumo: el ciudadano como consumidor*, en *Constitucionalismo crítico: liber amicorum Carlos de Cabo Martín*, Valencia, 2016, p. 489 ss.

⁴⁸ F. Balaguer Callejón, *Data protection and the transformation of rights in the digital society*, en *UNIO – EU Law Journal*, 10(1)/2024, p. 3 ss.

⁴⁹ K. Karimi, R. Fox, *Scrolling, sipping, and mobilizing: TikTok's influence over Generation Z's political behavior*, en *The Journal of Social Media in Society*, 12(1)/2023, pp. 199-200.

⁵⁰ M.A. Presno Linera, A. Meuwese, *La regulación de la inteligencia artificial en Europa*, en *Teoría y Realidad Constitucional*, 54/2024, p. 140.

⁵¹ J.G. Bullock, A.S. Gerber, S.J. Hill, G.A. Huber, *Partisan bias in factual beliefs about politics*, en *NBER Working Paper*, 19080/2013, pp. 27-30.

riales de búsqueda de los usuarios⁵². Este fenómeno intensificado por la emergencia de nuevas plataformas como TikTok, ha creado incluso una sección donde ya no aparecen los usuarios que sigues, sino un “para ti” en el que solo aparecen recomendaciones.

En estas recomendaciones se entremezcla una amplia gama de contenidos políticos, que aparecen no solamente con un tono serio sino camuflado a través de “memes” o con música⁵³, bombardeando al usuario de nuevo contenido dirigido o *targeted content*. Especialmente esto acontece en ciertos grupos poblacionales, como son los más jóvenes, la llamada Generación Z, donde acceden a un discurso político predominantemente seleccionado. Las elecciones presidenciales de 2024 en Estados Unidos se han visto condicionadas por la distribución masiva de vídeos que han influido en la intención de voto. Lo más preocupante de estos vídeos de entre 15 y 60 segundos es que han hecho que TikTok se convierta en la plataforma donde las nuevas generaciones se informen, creando una “brecha de información cada vez mayor a medida que las personas recurren a noticias más cortas y rápidas”⁵⁴. Esta plataforma supera incluso a Facebook y se sitúa a la par que Instagram en popularidad⁵⁵.

La emergencia de la IA también tiene otros efectos, entre ellos la trazabilidad, como consecuencia de la mayor autonomía y autoaprendizaje que permite generar un elevado número de recomendaciones, decisiones y contenidos sin supervisión directa; ello puede tener graves consecuencias para la opinión pública y los procesos electorales. En la actualidad es difícil identificar cómo un sistema algorítmico llega a determinadas conclusiones o recomendaciones, lo que impide detectar sesgos o manipulación durante las campañas electorales. Además, estas recomendaciones pueden tener un impacto social muy elevado al influir sobre la percepción de candidatos o partidos mediante generación masiva de contenido y, en particular, las *deepfakes*, las cuales se han intensificado a través de la generación de imágenes y discursos políticos mediante IA que, en numerosas ocasiones, son atribuidos a políticos reales, desdibujando la frontera entre la realidad y la ficción. Las consecuencias constitucionales son que el debate político se diluye, lo que provoca el aislamiento de los votantes y el refuerzo de ciertas posiciones políticas extremas. Al mismo tiempo, se produce una limitación de la diversidad de pensamientos y la búsqueda del consenso. Además, las figuras de referencia son conformadas por personajes públicos con tendencias ideológicas similares. De este modo, el desplazamiento de la deliberación hacia el espacio digital no equivale a su reproducción en otro medio, sino a su fragmentación. La política en red tiende a atomizar la esfera pública, sustituyendo la copresencia por la conexión, el debate por la interacción y la comunidad por la agregación⁵⁶. La difusión de desinformación puede suprimir la participación política, generando desconfianza hacia las instituciones e impidiendo la participación informada⁵⁷. En este sentido, las redes no son las nuevas plazas, sino espacios de circulación discursiva desanclados del tiempo y el lugar⁵⁸.

⁵² Como demostraron inicialmente estos autores con Facebook, como este conocimiento aumentaba la satisfacción con el producto que les aparecía en su *Feed*, M. Eslami, A. Rickman, K. Vaccaro, A. Aleyasen, A. Vuong, K. Karahalios, K. Hamilton, C. Sandvig, “I always assumed that I wasn’t really that close to [her]”: Reasoning about Invisible Algorithms in News Feeds, en *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 153-162.

⁵³ Los vídeos incluían desde el conflicto de Rusia, una campaña contra el uso de las mascarillas.

⁵⁴ K. Karimi, R. Fox, *Scrolling, sipping, and mobilizing*, cit., pp. 199-200.

⁵⁵ También la participación política se transforma hacia el *clicktivismo*, con acciones como compartir o dar “me gusta” que, gracias al *storytelling* y a referentes cercanos, conectan con los jóvenes. Aunque se cuestiona su impacto real y la sobreexposición informativa, estas plataformas actúan como catalizadores de movilización y concienciación rápida. Ejemplos representativos de movimientos activistas en redes: *Black Lives Matter (BLM)*, *Blackout Tuesday*, el movimiento feminista, y las protestas anticorrupción en Chile (2019). Véase: K. Karimi, R.L. Fox, *Scrolling, sipping, and mobilizing*, cit., p. 181 ss.; M.S. Hassan, S.N. Allam, Z.M. Azni, M.H. Khamis, *Social Media and Political Participation Among Young People*, en *Jurnal Sains Sosial*, 1/2016, p. 101 ss.

⁵⁶ S. Bagni, S. Baldin, F. Rinaldi, M. Rinaldi, G. Pavani, *La organización del Estado*, en L. Pegoraro, A. Rinella (dirs.), S. Ragone, (coord.), *Derecho constitucional comparado. Sistemas constitucionales*, Turín, 2022, vol. A, p. 100.

⁵⁷ De esta manera, ha concluido el Tribunal Europeo de Derechos Humanos (Sección Cuarta) en el *Caso Bradshaw y otros c. Reino Unido*, núm. 15653/22, 22 de julio de 2025.

⁵⁸ *Ibid.*

3. La respuesta normativa europea frente a los riesgos democráticos de las plataformas digitales y la inteligencia artificial

Las nuevas plataformas digitales están siendo el medio para la proliferación de estos fenómenos; como advierte Balaguer Callejón, al asentarse estas sobre modelos de negocio orientados a la captación del público con fines publicitarios y que muestran una tendencia al monopolio y oligopolio, no pueden ser verdaderos instrumentos de participación democrática⁵⁹. Sin embargo, en la actualidad es el espacio donde se producen la mayor parte de las comunicaciones y son esenciales a fin de que un partido político pueda continuar en el proceso electoral; para que tengan la potencialidad de ser verdaderos espacios para la participación democrática, es necesaria una intervención pública. Ante estos riesgos en las elecciones, el derecho público se ha visto en la necesidad de actualizar e incluso de crear nuevos conceptos; en este sentido, como ya advertía Sánchez Barrilao, el Derecho no puede seguir limitándose a ir al “rebufo del progreso tecnológico”⁶⁰. Además, esta nueva normativa no debe quedar confinada al ámbito territorial de un solo Estado, dada la naturaleza transnacional de los actores implicados en el ecosistema digital⁶¹.

En la actualidad, la dificultad del objeto – la IA – por su carácter tan técnico, ha planteado preocupaciones en torno al principio democrático y la garantía del pluralismo. Las nuevas respuestas regulatorias de la UE han pasado por fomentar más transparencia y rendición de cuentas en el espacio digital, así como la introducción del “*hard law*” europeo. Como ya advertía García Mahamut no se puede confiar únicamente “ni en la autorregulación empresarial, no digamos de las grandes tecnológicas, como medio eficaz, efectivo y en buena parte suficiente para garantizar los derechos en juego de los ciudadanos”⁶². En un primer momento, la UE reguló los riesgos del mundo digital a través de la protección de datos personales, especialmente con el Reglamento General de Protección de Datos⁶³ (en adelante RGPD), el cual estableció principios de licitud, transparencia y finalidad, prohibió el tratamiento de datos sensibles (como opiniones políticas o creencias ideológicas de acuerdo con el art. 9.1 RGPD) y solo lo permitió bajo estrictas excepciones (art. 9.2 RGPD), buscando así garantizar la privacidad y evitar usos abusivos de los datos, incluidos en contextos electorales.

Desde instituciones como la Organización para la Cooperación y el Desarrollo Económico (OCDE) se ha construido una serie de principios sobre Inteligencia Artificial en la declaración de 2019 y actualizados en 2024⁶⁴, señalando la necesidad de que la IA respetara los valores democráticos. Así, la Recomendación de la Unesco sobre ética de la Inteligencia Artificial (2021)⁶⁵ abogaba por la atención a los colectivos vulnerables y alfabetización digital, relevante para proteger el voto informado⁶⁶. También está el Convenio Marco del Consejo de Europa sobre IA, Derechos Humanos, Democracia y

⁵⁹ F. Balaguer Callejón, *Redes sociales, compañías tecnológicas y democracia*, en *Revista de Derecho Constitucional Europeo*, 32/2019, p. 1 ss.

⁶⁰ J.F. Sánchez Barrilao, *El Derecho constitucional ante la era de Ultrón: la informática y la inteligencia artificial como objeto constitucional*, en *Estudios de Deusto. Revista de Derecho Público*, 64(2)/2016, p. 225 ss.

⁶¹ S. Sassi, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, en *Analisi Giuridica dell'Economia*, 18(1)/2019, p. 109 ss.

⁶² R. García Mahamut. *Elecciones, protección de datos y transparencia en la publicidad política: la apuesta normativa de la UE y sus efectos en el ordenamiento español*, en *Revista española de la transparencia*, 17/2023, p. 103.

⁶³ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

⁶⁴ Véase el documento de la OCDE (<https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449>).

⁶⁵ Aprobada en noviembre de 2021 por consenso entre los 193 Estados miembros. Este es el primer instrumento normativo global en ética de IA.

⁶⁶ También, hay que señalar el proceso de IA de Hiroshima (2023) donde se reconoce la necesidad de mitigar los riesgos para proteger a los individuos, el Estado de Derecho y los valores democráticos a través de la creación de una serie de principios internacionales. Asimismo, La Declaración de Bletchley que establece una colaboración internacional para mitigar riesgos de IA; en ella se advierte sobre los riesgos de la IA en los procesos democráticos y la necesidad de garantizar pluralismo, transparencia y supervisión para evitar que estas tecnologías comprometan la integridad electoral. Véase: Declaración de Bletchley (2025), *The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023*, Policy Paper, actualizada el 13 de febrero de 2025 (<https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>).

Estado de Derecho⁶⁷ (2024) que es un tratado, aún en espera de plena ratificación. Este establece obligaciones para proteger derechos humanos y procesos democráticos frente a la IA, y crea mecanismos de cooperación, supervisión y recursos legales para gestionar riesgos y garantizar transparencia.

El *Digital Services Act*⁶⁸ vino a establecer a nivel europeo obligaciones sobre los proveedores de contenido en grandes plataformas digitales y motores de búsqueda. Para ello, sus artículos 34 y 35 DSA, determinan una obligación de evaluar riesgos sistémicos; en concreto, el art. 34.1.c DSA señala que se debe evaluar cualquier riesgo sistémico que produzca un “efecto negativo real o previsible sobre el discurso cívico y los procesos electorales, así como sobre la seguridad pública”. En consecuencia, los factores de riesgo sistémico relacionados con los procesos electorales incluyen la manipulación de la plataforma y la publicidad encubierta. El art. 35 DSA establece una obligación de aplicar medidas razonables, proporcionadas y eficaces para mitigar estos riesgos. Además, esta normativa introducía una serie de obligaciones de acuerdo con los arts. 27 y 38 de la DSA que exigen transparencia sobre los parámetros principales de los sistemas de recomendación y la opción de ofrecer sistemas sin personalización algorítmica⁶⁹. La publicidad política en línea específicamente es regulada en los arts. 36 y 39 DSA, donde se incluye una serie de obligaciones de transparencia en la publicidad, como es el envío de la publicidad política y el perfilado ideológico. Esto se complementa con los arts. 36 y 48 DSA que incluyen mecanismos de respuesta ante crisis provocadas, por ejemplo, por campañas masivas de desinformación o manipulación extranjera.

A raíz de esta situación, la Comisión, de acuerdo con el art. 35.3 del DSA, publicó una serie de directrices donde recomendó cómo mitigar los riesgos sistémicos *online* que pueden impactar en la integridad de las elecciones en la que incluyó la específica guía para las Elecciones Europeas de junio⁷⁰. En abril de 2024, la Comisión Europea utilizó sus nuevas facultades bajo la DSA, que están estrechamente vinculadas con el Reglamento de Inteligencia Artificial para realizar una prueba a plataformas como Google, Facebook, TikTok, YouTube, X, Snapchat, Instagram y Bing, coordinadores de servicios digitales y organizaciones de la sociedad civil para analizar cómo estaban preparadas frente a la manipulación electoral y la posible injerencia en las elecciones europeas⁷¹.

Estas pruebas consistían en una serie de escenarios ficticios que simulaban casos pasados. A la vista de estos fenómenos y con las próximas elecciones que estaban pendientes, las del Parlamento Europeo de 2024, este documento era un llamamiento a que las plataformas intentaran mitigar estos riesgos específicos. Teniendo en cuenta sus efectos en los derechos en el ámbito europeo como es la dignidad humana, el respeto a la vida privada y familiar, la protección de datos personales, la libertad de expresión e información – incluida la libertad y el pluralismo de los medios –, la libertad de asociación y la libertad de empresa en la Carta de los Derechos Fundamentales de la UE, esta ha sido criticada como “una suerte de regulación horizontal de los derechos, una intervención desde la lógica económica del mercado interior que puede llegar a desnaturalizarlos”⁷². Esta normativa, por

⁶⁷ El Convenio Marco sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho, que se abrió a la firma durante la conferencia de Ministros de Justicia del Consejo de Europa celebrada en Vilna el 5 de septiembre de 2024 y ha sido firmado por Andorra, Georgia, Islandia, Noruega, Moldavia, San Marino, el Reino Unido, Israel, Estados Unidos y la Unión Europea.

⁶⁸ Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, sobre un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (*Digital Services Act*).

⁶⁹ Tal como venía sido definido en el art. 4. 4 de la Reglamento (UE) 2016/679.

⁷⁰ Comisión Europea, [Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35\(3\) of Regulation](#) (EU) 2022/2065.

⁷¹ Comisión Europea, Stress tests on platforms' election readiness under the Digital Services Act (<https://digital-strategy.ec.europa.eu/es/news/commission-stress-tests-platforms-election-readiness-under-digital-services-act>).

⁷² Á. Barredo Artíguez, *El Reglamento Europeo de Servicios Digitales y la defensa de la democracia*, en *Revista de Derecho Político*, 122/2025, p. 295 ss.

otra parte, también debe tener en cuenta el Reglamento (UE) 2024/900 sobre Publicidad Política que impone obligaciones adicionales de transparencia y orientación⁷³.

Otra de las prácticas que han sido explícitamente prohibidas a las plataformas digitales es la posibilidad de que manipulen al usuario mediante prácticas conocidas como *nudging* “arquitectura de elección”, que limiten su autonomía o desinformen (considerando 67). Dichos *nudges* inaceptables son aquellos que distorsionan o interfieren con la capacidad del usuario para tomar decisiones informadas, aumentan la dificultad para revertir una acción tomada o utilicen configuraciones predeterminadas difíciles de cambiar. El Parlamento Europeo, además, hizo un llamamiento para prohibir técnicas de *nudging* adictivo, como el *scrolling* infinito o la reproducción automática (*autoplay*), y para crear un “derecho a no ser molestado” en redes sociales. Asimismo, propuso elaborar una lista de recomendaciones, como “piensa antes de compartir”, “desactivar las notificaciones por defecto”, “usar *feeds* cronológicos” o “activar el modo en escala de grises”⁷⁴. Ante esto se ha propuesto el *Digital Fairness Act*⁷⁵, que es un proyecto que busca prevenir prácticas manipuladoras en entornos digitales.

La aplicación de la DSA durante las elecciones al Parlamento Europeo incluyó mecanismos de identificación y etiquetado de contenido generado por IA, así como protocolos de actuación ante amenazas inmediatas. En el caso de las elecciones presidenciales de Rumanía, “TikTok permitió la promoción de contenido y la difusión de mensajes políticos a través de influencers y cuentas coordinadas sin el etiquetado adecuado, lo que contradecía las obligaciones legales”⁷⁶, ante esto la Comisión Europea activó la *maquinaria pesada* prevista en la DSA. En primer lugar, impuso una orden de retención de datos a TikTok el 5 de diciembre de 2024 para preservar la información clave relacionada con riesgos sistémicos durante el proceso electoral; esto incluyó datos sobre sistemas de recomendación y cuentas falsas, fundamentado en el art. 67 de la DSA. Este permitió a la Comisión solicitar la preservación de datos para evaluar el cumplimiento del reglamento; los problemas que siguen presentándose se encontraron en un acceso insuficiente a los datos, lo que hizo que se tuviera que recurrir al art. 40 DSA y por eso se han propuesto mejorar la transparencia sobre los datos que las plataformas recopilan, interfieren y procesan⁷⁷.

Además, se abrió el 17 de diciembre de 2024 un procedimiento formal contra TikTok por las posibles violaciones de la DSA en el caso de las elecciones de Rumanía en cuanto su obligación de gestionar riesgos sistémicos relacionados con la integridad electoral de acuerdo con el art. 34.1 y 2 que establecen una evaluación y gestión de dichos riesgos sistémicos. Asimismo, se sigue investigando si la plataforma cumplió con las obligaciones de transparencia sobre publicidad política como las mencionadas en el art. 26 de la DSA y el acceso a los datos que establece el art. 39 de la DSA. En el ámbito comparado, la Corte Constitucional de Rumanía ha ido más allá al considerar la desinformación como un auténtico “parámetro de violación del Estado de derecho, anulando el procedimiento electoral”⁷⁸, en coherencia con el principio del artículo 5.1 del Reglamento de IA, que prohíbe los sistemas destinados a manipular procesos democráticos.

Finalmente, ante la aparición de la IA, la respuesta jurídica de la Unión Europea frente a este nuevo desafío ha sido compatibilizar el desarrollo tecnológico con la garantía de los derechos fundamentales,

⁷³ Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política.

⁷⁴ Parlamento Europeo, *New EU rules needed to make digital platforms less addictive*, 2023 (<https://www.europarl.europa.eu/news/en/press-room/20231023IPR08161/new-eu-rules-needed-to-make-digital-platforms-less-addictive>).

⁷⁵ Ahora mismo esta iniciativa se encuentra en fase de evaluación (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14622-Digital-Fairness-Act_en).

⁷⁶ A. Seceleanu, B. I. Garabet, *Communication psychopathologies in the presidential election campaign in Romania*, en *Revista de Științe Politice. Revue des Sciences Politiques*, 86/2025, p. 25.

⁷⁷ C. Goanta, S. Zannettou, R. Kaushal, J. van de Kerkhof, T. Bertaglia, T. Annabell, H. Gui, G. Spanakis, A. Iamnitci, *The Great Data Standoff: Researchers vs. Platforms Under the Digital Services Act*, Working Paper, 2025.

⁷⁸ A. Sterpa, S. Sassi, *La Corte costituzionale della Romania difende la democrazia liberale dalla disinformazione. Prime note sulla sentenza n. 32 del 6 dicembre 2024*, en *federalismi.it*, 4/2025, p. 163. El artículo hace referencia a la Sentencia de la Corte Constitucional de Rumanía, *Sentencia n.º 32, de 6 de diciembre de 2024*.

el pluralismo, el Estado social y de derecho sobre estos principios –transparencia, la rendición de cuentas y la intervención humana adecuada –, a la par que promover la innovación y la competitividad⁷⁹. En este contexto, ha aparecido la regulación europea clave, el Reglamento UE 2024/1689 sobre Inteligencia Artificial (en adelante, el RIA), donde se establecen normas armonizadas para el uso de IA, incluidos sistemas generativos aplicados a procesos electorales. Esta normativa establece un enfoque basado en riesgos; es decir, prohíbe usos de IA que pongan en peligro derechos fundamentales, como el derecho al voto o la democracia. Además, este se aplicará a sistemas de IA desarrollados fuera de la UE pero que sean usados por ella. Esta nueva regulación busca evitar que la IA se utilice para manipular, discriminar o vulnerar derechos políticos. De esta manera, las autoridades nacionales y europeas tendrán competencia para vigilar el uso de la IA en las campañas y plataformas digitales. Por otra parte, se establecen obligaciones de transparencia y responsabilidad de los proveedores de IA, lo que es clave para luchar contra la desinformación electoral.

El Preámbulo del RIA subraya que esta inferencia es lo que permite a la IA generar efectos en la comunicación política y, por tanto, lo que plantea riesgos directos para el pluralismo democrático. El RIA define como característica esencial de la IA su capacidad de inferencia; es decir, producir predicciones, contenidos, recomendaciones o decisiones a partir de los datos recibidos (art. 3 RIA)⁸⁰, señalando que esa capacidad puede influir en entornos físicos o virtuales, como el debate público en redes sociales o los procesos electorales. Además, este Reglamento establece como prácticas prohibidas el uso de IA de acuerdo con el art. 5.1 del RIA, las que puedan manipular o interferir en procesos democráticos.

En esta situación ya compleja, donde tres normativas afectan de manera indirecta a la propaganda política, es crucial destacar la nueva propuesta de reforma del Reglamento sobre la financiación de partidos políticos europeos y fundaciones⁸¹, presentada por la Comisión, la cual también incluye propuestas para prevenir la financiación de cierta publicidad política que suponga el tratamiento de datos de los usuarios en las plataformas digitales. En este contexto, la opinión del Tribunal de Cuentas Europeo afirmó que “existe un riesgo de solapamiento de competencias, por ejemplo, en lo que respecta al control de las normas relacionadas con la publicidad política”⁸².

Paralelamente se está intentando blindar la libertad de prensa, a través de nueva normativa; es el nuevo Reglamento Europeo sobre la libertad de los Medios de Comunicación (2024)⁸³, que pretende garantizar el pluralismo y la independencia de los medios. Además, se va a constituir como una norma comunitaria fundamental para los medios de comunicación en el contexto digital, como se ha señalado, a fin de que “puedan operar más fácilmente a través de las fronteras en el mercado interior de la UE, sin presiones indebidas y teniendo en cuenta la transformación digital del espacio mediático”⁸⁴. Recientemente, el TEDH ha recordado en el asunto *Bradshaw y otros c. Reino Unido*, que los Estados no pueden permanecer pasivos ante pruebas de que sus procesos democráticos están amenazados, pero que existe un amplio margen para contrarrestar estas amenazas. También, recordando que cualquier regulación debe equilibrarse con la libertad de expresión, sobre todo en los días previos a las elecciones.

⁷⁹ M. A. Presno Linera, A. Meuwese, *La regulación de la inteligencia artificial en Europa, en Teoría y Realidad Constitucional*, 54/2024, p. 156.

⁸⁰ *Ibid.*, p. 141.

⁸¹ Se ha alcanzado un acuerdo político provisional en junio de 2025 entre Parlamento Europeo y Consejo para reformar el reglamento vigente y fortalecer la transparencia, reducir la burocracia y mejorar la capacidad de respuesta ante riesgos de interferencia extranjera en el ámbito político europeo. Véase: Parlamento Europeo y Consejo, *Acuerdo político provisional sobre partidos y fundaciones políticas europeas*, junio 2025 (<https://www.europarl.europa.eu/news/en/press-room/20250613IPR28914/deal-on-new-rules-for-european-political-parties-and-foundations>).

⁸² [Dictamen 01/2022. sobre la propuesta de la Comisión de Reglamento sobre el estatuto y la financiación de los partidos políticos europeos y las fundaciones política europeas](#), apartado 45.

⁸³ Reglamento (UE) 2024/1083 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se establece un marco común para los servicios de medios de comunicación en el mercado interior y se modifica la Directiva 2010/13/UE.

⁸⁴ C. Pauner Chulvi, *La protección de las fuentes periodísticas en la era digital y el impulso regulatorio de la Unión Europea, en Teoría y Realidad Constitucional*, 54/2024, p. 203.

4. El etiquetado obligatorio y sanciones por contenido Inteligencia Artificial no identificado en España e Italia

En el ámbito nacional, la normativa española también trató de adaptar el marco de los partidos políticos a la realidad digital a través de la disposición final tercera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que introdujo el art. 58 bis en la Ley Orgánica del Régimen Electoral General (LOREG, 1985). Sin embargo, en su redacción final resultó legítimar “el tratamiento de opiniones políticas por parte de los partidos. Además, admitía la elaboración sistemática y exhaustiva de perfiles electorales, así como el envío de propaganda mediante microsegmentación”⁸⁵. Esta disposición también fue criticada por su laxidad frente a la posibilidad de recopilación y tratamiento de opiniones políticas en el marco de las elecciones, por lo que fue objeto de recurso de inconstitucionalidad promovido por el Defensor del Pueblo.

Esta propuesta fue modificada ante las críticas de los grupos parlamentarios y amplios sectores de opinión pública. Sin embargo, aunque fue cambiada también fue objeto de un proceso constitucional, ante los temores de amparar el perfilado o el *microtargeting*; aunque el Tribunal Constitucional no se pronunció expresamente sobre estas cuestiones, sí que entendió que era contrario a la Constitución por no establecer las necesarias garantías adecuadas en la propia ley, vulnerando la reserva de ley (art. 53.1 CE), el contenido esencial al derecho fundamental que se desprende del art. 18.4 CE a la protección de datos al no delimitar los usos permitidos de los datos, y señaló que no se identificaba en qué consistía el interés público⁸⁶. Hasta la fecha, no se ha aprobado ninguna reforma de la LOREG que sustituya el apartado 1 del artículo 58 bis, declarado inconstitucional por la STC 76/2019, de 22 de mayo⁸⁷. Además, tras las últimas elecciones de 2021 se ha alertado por el Tribunal Supremo en la sentencia n. 735/2022⁸⁸ – donde se analizaba el cierre del perfil de Vox-Cataluña en Twitter – que existe un vacío legal respecto a la regulación de las plataformas digitales, lo que llevó a que en última instancia hayan sido las propias plataformas las que actúen como “juntas electorales paralelas”⁸⁹ a través de decisiones automatizadas para poder suspender a partidos, coaliciones o candidaturas.

Al mismo tiempo, ante los riesgos de la comunicación política digital y al uso intensivo de datos en campañas electorales, España ha dado un nuevo paso con la aprobación el 11 de marzo, por el Consejo de Ministros, del anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial (Anteproyecto de Ley de IA), que desarrolla el régimen sancionador y de gobernanza previsto en el Reglamento (UE) 2024/1689 o RIA⁹⁰. De esta forma, se introducen normas armonizadas para la introducción en el mercado, la puesta en funcionamiento y la utilización de sistemas de IA en el contexto español. En nuestro caso, es interesante las novedades que introducen en el régimen general y en el procedimiento sancionador, según se viene a mostrar.

En esta propuesta se concreta el régimen de infracciones de acuerdo con el art. 99 RIA. Entre las cuestiones que se introducen es una obligación de transparencia en consonancia con el art. 50 RIA; en concreto, en el art. 16 del anteproyecto tipifica como infracción grave para los proveedores de sistemas de IA el incumplimiento de la obligación de etiquetar correctamente cualquier imagen, audio o vídeo generado o manipulado con IA que constituya una ultrasuplantación (*deepfake*) electoral, manipulaciones subliminales y uso indebido de datos que cree cualquier texto destinado a informar al público sobre asuntos de interés público, así como el incumplimiento de la obligación de comunicar a

⁸⁵ D.J. Villares, *La inconstitucional habilitación a los partidos políticos para recabar datos sobre opiniones políticas. Comentario a la STC 76/2019, de 22 de mayo*, en *Revista española de derecho constitucional*, 121/2021, p. 303 ss.

⁸⁶ STC 76/2019, de 22 de mayo.

⁸⁷ D. Jove Villares, *La inconstitucional habilitación a los partidos políticos para recabar datos sobre opiniones políticas. Comentario a la STC 76/2019, de 22 de mayo*, en *Revista Española de Derecho Constitucional*, 121/2021, p. 303 ss.

⁸⁸ Sentencia n. 735/2022, de 28 de febrero de 2022, ECLI:ES:TS:2022:735.

⁸⁹ L. Corredoira y Alfonso, *Garantías de la libertad de expresión en redes sociales y medios. Doctrina de la Junta Electoral Central durante los comicios españoles celebrados en 2023*, en *Revista de Derecho Político*, 120/2024, p. 209 ss.

⁹⁰ Anteproyecto de ley el buen uso y la gobernanza de la Inteligencia Artificial (<https://avance.digital.gob.es/layouts/15/HttpHandlerParticipacionPublicaAnexos.ashx?k=19128>).

las personas de que están interactuando con un sistema de IA. De esta manera, se busca una prevención de la manipulación a través de la ley que habilita a la Agencia Española de Supervisión de la Inteligencia Artificial (en lo sucesivo AESIA) y a las autoridades de vigilancia para retirar o bloquear IA usada en campañas si se considera un riesgo inaceptable. Además, se refuerza la trazabilidad y la responsabilidad en el uso de IA que pueda influir en el debate público o en el acceso igualitario a la información; para garantizarlo se proveen canales de denuncia ciudadana como el previsto en el art. 29 Anteproyecto, de modo que cualquier persona puede alertar sobre IA utilizada de forma ilícita en un proceso electoral.

Este canal externo anónimo será creado por la AESIA para que cualquier persona física pueda informar de infracciones de esta ley, como en los casos de procesos electorales. La AESIA decidirá en 10 días si abre procedimiento o remite a la autoridad competente. En el caso electoral, sería la Junta Electoral Central, según el art. 6.6 del Anteproyecto; de acuerdo con este artículo, se designan a las autoridades de vigilancia del mercado. En concreto, el apartado sexto de este artículo designa a la Junta Electoral Central (en adelante, JEC) como autoridad de vigilancia del mercado para los sistemas de IA de alto riesgo descritos en el Anexo III.8.c) RIA, que son los relacionados con procesos democráticos y prácticas prohibidas de IA que afecten a elecciones. De esta manera, si se detectara un sistema de IA que puede manipular el voto, influir indebidamente en la opinión pública o vulnerar principios democráticos, la JEC tendrá competencia para inspeccionar, sancionar y, en casos graves, ordenar su retirada inmediata. Se permitirán actuaciones previas para recabar información y medidas provisionales para evitar daños a derechos fundamentales durante la tramitación, entre las que se incluye la retirada o desconexión de un sistema de IA si se considera que presenta un riesgo inaceptable, incluso antes de que haya una resolución final. Lo que todavía no está claro es cómo se conjugará eso con la actividad de la AESIA⁹¹, que es el organismo al que se le atribuye la potestad sancionadora en la mayoría de las prácticas prohibidas, así como en los sistemas de alto riesgo contemplados en el anexo III del RIA. Cabe señalar que algunas de estas prácticas no afectan directamente a los procesos electorales, sino que lo hacen de manera indirecta, lo cual genera cierta ambigüedad en cuanto a las competencias que asumirá la JEC y cuáles, la AESIA.

De esta forma, la AESIA actúa como punto de contacto único y puede asumir la supervisión si la autoridad sectorial (como la JEC) no dispone de medios suficientes, lo que puede afectar a las competencias de la JEC. Por este motivo se prevé un deber de colaboración entre autoridades nacionales, la Comisión Europea y organismos especializados en los casos de incidentes graves recogido en el art. 8 Anteproyecto IA. Las autoridades de vigilancia deben informar de incidentes graves a nivel nacional y europeo en máximo 72 horas a través del sistema *Safety Gate*, de acuerdo con el art. 8. 2. d) Anteproyecto. Si el riesgo excede el territorio nacional, se establece un deber de comunicar medidas correctoras y provisionales a la UE para que la respuesta sea lo más coordinada posible. Se prevé la posibilidad de Comisión Mixta de Coordinación presidida por la AESIA junto con las autoridades competentes para asegurar la actuación uniforme y rápida.

En el art. 10.1 Anteproyecto – como ya establecía el RIA en el art. 5.1 párrafos a), b), c), d), e), f) y g)– se reconocen una serie de prácticas prohibidas en los procesos democráticos. De esta forma, en el caso de que el uso de IA influya de forma sustancial en elecciones alterando el comportamiento de los votantes de manera engañosa o coercitiva quedará expresamente prohibida. La prohibición es absoluta, pues no está sujeta a excepciones como en el caso de la biometría para fines de seguridad; y esto incluye tanto el uso como la comercialización o puesta en servicio de dichos sistemas. Estas prácticas prohibidas se consideran una infracción muy grave de acuerdo con el art. 14.1 a) Anteproyecto

⁹¹ Esta agencia fue creada por Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial (<https://www.boe.es/buscar/doc.php?id=BOE-A-2023-18911>). Junto con la Dirección General de Inteligencia Artificial que es la competente en regulación y supervisión y la Secretaría de Estado de Digitalización e Inteligencia Artificial, la cual lidera el desarrollo normativo sobre IA. Además, se ha establecido un Plan nacional España Digital 2025 / 2026 y Estrategia Nacional de Inteligencia Artificial (ENIA) que plantean un desarrollo ético, inclusivo y alineado con la Carta de Derechos Digitales y la Estrategia de IA 2024, uno de los ejes será Desarrollar IA transparente, responsable y humanística (clave para procesos democráticos).

y llevan aparejadas sanciones muy altas (art. 13.1. a), como se especifica entre 7.500.001 € y 35.000.000 € o entre 2% y 7% del volumen de negocios global, si es mayor. Aunque aquí no se menciona expresamente la JEC, sí está claro que cualquier sistema de IA que se use para manipular o interferir en elecciones cae en la categoría de práctica prohibida (art. 10.1) y, si se utiliza, se considera infracción muy grave (art. 14.1.a).

El Anteproyecto también introduce como infracciones graves supuestos como el incumplimiento de la obligación de marcar contenidos, como textos o audios generados por inteligencia artificial, de acuerdo con el art. 16.1 del Anteproyecto de IA. Además, los casos en que se genere o manipule contenido, como *deepfakes*, para influir en la opinión pública sobre asuntos de interés general, se califican como infracciones muy graves, conforme al art. 20 del mismo Anteproyecto. De esta forma, se establecen obligaciones específicas para prevenir la manipulación electoral, entre ellas la de identificar los contenidos artificiales y garantizar que los sistemas que generen *deepfakes* marquen sus resultados para que sean detectables como no reales.

Por un lado, se introducen las evaluaciones de impacto sobre derechos fundamentales obligatorias cuando se use IA de alto riesgo en contextos democráticos. Además, la implementación de *sandboxes* regulatorios en España y la creación de una serie de directrices prácticas. Hay que añadir que desde 2023 funciona el *sandbox* regulatorio nacional que permite mediante la experimentación controlada realizar evaluaciones de las aplicaciones de IA, donde además se incluyen aquellas que puedan afectar a las elecciones y se permite verificar si se cumplen las obligaciones legales sin riesgo inmediato de sanción administrativa⁹².

Por otro lado, en Italia, se ha aprobado el proyecto de Ley de Inteligencia Artificial, aprobada el 17 de septiembre por el Parlamento, conocido como “AI Bill”, el cual delega en el Gobierno la adopción, dentro de doce meses, de un decreto legislativo que adopte también el Reglamento de IA⁹³. El AI Bill establece obligaciones clave para el desarrollo de sistemas y modelos de IA, destacando la importancia de respetar la autonomía humana y la toma de decisiones. Afirma que la IA no debe socavar la estructura democrática de la vida institucional y política. El último caso reciente, ha vuelto a poner en el centro del debate esta cuestión. El partido La Liga difundió imágenes generadas por IA en redes sociales, donde representaba a personas migrantes como criminales y amenazas públicas. Este caso ha sido trasladado a la *Autorità per le Garanzie nelle Comunicazioni* de Italia (Agcom). En relación con estos hechos, X ha declarado que no se encuentra legalmente obligada a etiquetar la totalidad del contenido generado por inteligencia artificial, calificando estos mensajes de La Liga como propaganda política evidente⁹⁴. Por su parte, Meta, propietaria de Facebook e Instagram, no emitieron ningún pronunciamiento público. De confirmarse la gravedad de los hechos, la Agcom podría imponer medidas sancionadoras en el marco de la Ley de Servicios Digitales de la Unión Europea.

En la legislación italiana, además, el art. 26 de la *Legge* n. 132/2025 sobre inteligencia artificial recoge modificaciones a diversos artículos del *Codice Penale* y del *Codice Civile*. En particular, el art. 294 del *Codice Penale*, titulado “*Attentati contro i diritti politici del cittadino*”, ha sido reformado para prever expresamente una agravante cuando el engaño se lleva a cabo mediante sistemas de inteligencia artificial: ahora establece que quien, con violencia, amenaza o engaño, impida total o parcialmente el ejercicio de un derecho político o induzca a alguien a ejercerlo contra su voluntad será sancionado con reclusión de uno a cinco años, y la pena se eleva a dos a seis años si dicho engaño se realiza utilizando

⁹² Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (https://www.boe.es/diario_boe/txt.php?id=BOE-A-2023-22767). En abril de 2025 se seleccionaron los primeros 12 proyectos que participan en este sandbox, cuyos resultados se usan como base para formular buenas prácticas y políticas regulatorias futuras. *Sandboxes* de IA (<https://espanadigital.gob.es/lineas-de-actuacion/sandbox-regulatorio-de-ia>).

⁹³ *Legge* n. 132 de 23 de septiembre de 2025 (*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*), publicada en la *Gazzeta ufficiale* el 25 de septiembre de 2025.

⁹⁴ Véase: <https://www.theguardian.com/technology/2025/apr/18/italian-opposition-complaint-far-right-matteo-salvini-lega-racist-ai-images>.

IA⁹⁵. Esta modificación no actúa como una norma electoral *per se*, pero tiene un impacto directo sobre la integridad de los procesos electorales al proteger la libertad de voto y prevenir mecanismos tecnológicos de manipulación.

5. Conclusiones

Las elecciones como núcleo de los sistemas democráticos necesitan un constitucionalismo que se anuncie como digital y que pueda ser operativo frente a los nuevos retos y problemas, especialmente en los derechos de participación política y a la propia democracia que tiene como pilar al pluralismo político; un constitucionalismo detenido en tiempos pasados no puede cumplir una de sus funciones principales como es ordenar el poder⁹⁶. Para ello, las nuevas normativas deben adaptarse a este nuevo entorno con una característica esencial que cambia a un ritmo muy rápido.

Este espacio fue en un inicio pensado como una oportunidad de mayor participación de los ciudadanos, como un “espacio de comunicación multimodal”⁹⁷. Sin embargo, la realidad ha mostrado la necesidad de intervención, porque, aunque sean de titularidad privada – como señala Vázquez Alonso – su función en el ámbito público digital les otorga una dimensión que trasciende lo meramente empresarial⁹⁸. Desde una perspectiva jurídica, el artículo evidencia que la opacidad en el uso de algoritmos y sistemas de inteligencia artificial en la publicidad política personalizada, sin mecanismos efectivos de transparencia y trazabilidad, puede vulnerar derechos y principios constitucionales como el pluralismo político, el derecho a un voto libre e informado y dificulta el control público; configurando prácticas prohibidas por el art. 5.1 del Reglamento (UE) 2024/1689 y el art. 10 del Anteproyecto de Ley de IA, sancionables como infracciones muy graves.

En cuanto a la normativa, a nivel europeo, puede señalarse que el *Digital Services Act* introduce, en materia electoral, un marco jurídico específico que obliga a las grandes plataformas y motores de búsqueda a evaluar y mitigar riesgos sistémicos que puedan afectar al discurso cívico y a la integridad de los procesos electorales (art. 34.1.c DSA), así como a aplicar medidas razonables y proporcionadas para reducir dichos riesgos (art. 35 DSA). Esta norma exige, además, transparencia reforzada en la publicidad política y en los sistemas de recomendación, incluyendo la obligación de identificar claramente los anuncios con relevancia electoral y prohibir técnicas manipuladoras como el *nudging* adictivo o el *scrolling* infinito en determinados contextos. El RIA adopta un enfoque basado en el riesgo, prohibiendo de forma expresa los usos de IA que puedan manipular procesos democráticos o influir sustancialmente en elecciones o referendos de manera engañosa o coercitiva (art. 5.1 RIA). Asimismo, impone obligaciones específicas de transparencia (art. 50 RIA) y de evaluación de impacto sobre derechos fundamentales cuando se utilicen sistemas de IA de alto riesgo en contextos democráticos (anexo III.8.c).

En relación con la aplicación práctica del DSA y del RIA en procesos electorales, cabe destacar el caso de Rumanía en 2024, donde la Comisión Europea activó las facultades previstas en la Ley de Servicios Digitales para preservar datos de TikTok y evaluar su cumplimiento en la gestión de riesgos sistémicos vinculados a la integridad electoral. Se investigó si la plataforma había cumplido con las obligaciones de transparencia sobre publicidad política y con la mitigación de riesgos como la desinformación, la injerencia extranjera y la manipulación algorítmica. Sin embargo, persisten desafíos como el acceso insuficiente a datos por parte de supervisores, la detección tardía de campañas de

⁹⁵ De esta forma se establece que: “*La pena è della reclusione da due a sei anni se l'inganno è posto in essere mediante l'impiego di sistemi di intelligenza artificiale*” (Art. 294).

⁹⁶ J.F. Sánchez Barrilao, *Constitucionalismo digital: entre realidad digital, prospectiva tecnológica y mera distopía constitucional*, en F. Balaguer Callejón (coord.), *Derechos fundamentales y democracia en el constitucionalismo digital*, Cizur Menor, 2023, p. 93 y ss.

⁹⁷ M. Castells, *Comunicación, poder y contrapoder*, cit., p. 13 y p. 21.

⁹⁸ V.J. Vázquez Alonso, *La obsolescencia probable*, cit.

manipulación y la necesidad de una cooperación internacional más efectiva para frenar prácticas transfronterizas que ponen en peligro el pluralismo político y la igualdad informativa.

A nivel nacional, en el caso del Anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial en España, uno de los elementos más novedosos en materia electoral es que, por primera vez en la normativa española, se designa expresamente a la JEC como autoridad de vigilancia del mercado para sistemas de IA de alto riesgo vinculados a procesos democráticos (Anexo III.8.c) RIA). Esto le otorga competencias no solo sancionadoras, sino también preventivas, incluyendo la retirada cautelar o desconexión inmediata de sistemas de IA que supongan un riesgo inaceptable para la integridad electoral, incluso antes de la resolución final. Además, se introduce una obligación de etiquetado de todo contenido artificial – ya sean imágenes, vídeos, audios o textos – con relevancia electoral, generados o manipulados por IA, y la posibilidad de activar canales de denuncia ciudadana anónima para alertar sobre usos ilícitos de IA en campañas, reforzando así la trazabilidad, la transparencia y la reacción rápida frente a la manipulación digital del voto.

No obstante, el nuevo marco plantea riesgos derivados de la posible coexistencia de competencias entre la Agencia Española de Supervisión de la Inteligencia Artificial y la Junta Electoral Central, lo que introduce retos de coordinación institucional que podrían afectar a la eficacia de la supervisión y la sanción. Para mitigar estos riesgos, resulta necesario reforzar las obligaciones de etiquetado, trazabilidad y evaluación de impacto, así como garantizar un acceso adecuado a los datos con el fin de prevenir y corregir manipulaciones electorales, en coherencia con el enfoque basado en el riesgo del *AI Act* y los principios del *Digital Services Act*.

Por su parte, Italia ha aprobado recientemente su *AI Bill*, que refuerza la protección al establecer un sistema de supervisión y dotar a la Agcom de nuevas competencias. Además, adopta un enfoque centrado en las personas, introduciendo sanciones en casos de difusión de imágenes o vídeos generados con IA ante el uso indebido de esta tecnología. Asimismo, la reforma del artículo 294 del *Codice Penale* introduce una agravante cuando el engaño político se comete mediante IA, fortaleciendo la protección de la libertad de voto y la integridad de los procesos electorales.

Para terminar, la situación de crisis que vive la democracia no es solo consecuencia de la IA, pero esta está incrementando los problemas que ya se advertían en nuestros sistemas políticos. Estos se han visto envueltos en nuevos escándalos que potencian la desconfianza hacia el sistema y hace que corrientes autocráticas tengan más fuerza⁹⁹. Si bien los inicios de Internet y las redes sociales despertaron la esperanza de convertirse en vías para proporcionar foros más amplios de deliberación y una vía para reforzar las democracias. El informe para la Democracia 2024 ha señalado que en la actualidad se ha producido un cambio de perspectiva¹⁰⁰. En él, se alerta la proliferación del discurso de odio y la desinformación, alimentando una polarización creciente, convirtiéndose en un arma también para la represión paradójicamente¹⁰¹. El derecho es fundamental para controlar estos nuevos procesos y mejorar la calidad de los procesos electorales; en este punto, la formación de una opinión en el voto es esencial y las nuevas regulaciones europeas son, junto al derecho nacional, fundamentales para garantizar la transparencia en estos procesos y regular una cuestión tan delicada como la propaganda política.

Abstract

Este artículo analiza cómo las plataformas digitales y los motores de búsqueda, impulsados por algoritmos y sistemas de IA cada vez más predictivos, reconfiguran el espacio público y generan riesgos sistémicos para la integridad

⁹⁹ J.F. Sánchez Barrilao, *El Impacto de la Inteligencia Artificial*, cit.

¹⁰⁰ *Democracy Report 2024: Democracy Winning and Losing at the Ballot*, V-Dem Institute Varieties of Democracy Institute (V-Dem), Universidad de Gothenburg, 2024, pp. 44-45, (https://www.v-dem.net/documents/44/v-dem_dr2024_highres.pdf).

¹⁰¹ *Ibid.*

electoral y el pluralismo político. Se abordan fenómenos como desinformación, deepfakes, la microsegmentación, el perfilado ideológico y el refuerzo de filter bubbles y echo chambers, amplificadas por las dinámicas de scrolling y recomendación en nuevas plataformas como TikTok. En el plano regulatorio, se examinan las regulaciones a nivel europeo como la Ley de Servicios Digitales; así como el enfoque del Reglamento de IA, que prohíbe usos manipuladores y refuerza la trazabilidad de contenido. También, se analiza el Anteproyecto de Ley de IA español, que impone el etiquetado obligatorio de contenidos generados por IA con relevancia pública, canales de denuncia y otorga funciones de supervisión a la Junta Electoral Central, sí como la nueva Ley Italiana, orientada a garantizar la transparencia algorítmica, que introduce nuevas sanciones y refuerza los marcos legales.

Palabras clave: inteligencia artificial, plataformas digitales, integridad electoral, transparencia algorítmica, regulación digital

*

This article analyzes how digital platforms and search engines, driven by increasingly predictive algorithms and AI systems, are reshaping the public sphere and creating systemic risks for electoral integrity and political pluralism. It addresses phenomena such as disinformation, deepfakes, microtargeting, ideological profiling, and the reinforcement of filter bubbles and echo chambers, amplified by scrolling and recommendation dynamics on emerging platforms like TikTok. On the regulatory level, it examines European initiatives such as the Digital Services Act and the AI Act's risk-based approach, which prohibits manipulative uses and strengthens content traceability. It also analyzes Spain's Draft AI Law, which mandates the labeling of AI-generated content of public relevance, establishes reporting channels, and grants supervisory powers to the Central Electoral Board, as well as Italy's new AI Law, aimed at ensuring algorithmic transparency, introducing new sanctions, and reinforcing legal frameworks.

Key words: artificial intelligence, digital platforms, electoral Integrity, algorithmic transparency, digital regulation