EL USO DE LA INTELIGENCIA ARTIFICIAL EN LAS CAMPAÑAS ELECTORALES Y SUS EFECTOS DEMOCRÁTICOS

RAFAEL RUBIO

SUMARIO

1. La tecnología electoral y su uso en campaña; 2. La amenaza tecnológica; 3. La digitalización de la información (y la desinformación) electoral; 4. Usos de la IA en las campañas electorales; 5. Primeras respuestas. 5.1 Autoregulación, 5.2 Respuesta legislativa, 5.3 La respuesta de los organismos electorales, 6. Conclusiones.

Fecha recepción:19.06.2024
Fecha aceptación: 29.10.2024

EL USO DE LA INTELIGENCIA ARTIFICIAL EN LAS CAMPAÑAS ELECTORALES Y SUS EFECTOS DEMOCRÁTICOS[1]

RAFAEL RUBIO[2]

El diseño de la tecnología es también el diseño de la sociedad. La aceleración tecnológica, el auge de las redes sociales, la minería de datos, el aumento de la capacidad de almacenamiento, la mejora exponencial de la capacidad del procesamiento de información y la automatización de procesos creativos en diferentes soportes, conduce a la progresiva virtualización de la realidad. Estos cambios afectan no sólo a la política, a través de la "digitalización de las conversaciones públicas", sino también a la sociedad, transformándola y provocando la acelerada virtualización de tareas y procesos sociales sensibles. Como advertía Castells hace ya muchos años la "revolución tecnológica, centrada en torno a la información, transformó nuestro modo de pensar, de producir, de consumir, de comerciar, de gestionar, de comunicar, de vivir, de hacer la guerra y de hacer el amor"[3].

Las amenazas tecnológicas a la democracia llevan años en la agenda pública. Si se depositaron inicialmente grandes esperanzas en la capacidad renovadora de las tecnologías digitales, ahora se experimenta una decepción a la que acompañan señales de

[1] Realizado con el apoyo del Proyecto de Investigación "Garantías institucionales y regulatorias. Autoridades electorales y de supervisión digital ante interferencias, narrativas hostiles, publicidad segmentada y polarización" (2023-2026) financiado en el marco de los Proyecto de Generación de conocimiento 2022. Referencia:

PID2022-137245OB-I00A.

Este artículo sintetiza el libro Inteligencia Artificial y Campañas electorales algorítmicas. Disfunciones informativas y amenazas sistémicas de la nueva comunicación política. Centro de Estudios Políticos y Constitucionales (2024).

[2] Catedrático de Derecho Constitucional de la Universidad Complutense, Departamento de Derecho Constitucional. Facultad de Derecho. Universidad Complutense de Madrid. Ciudad Universitaria. 28040 Madrid. Email: rafa.rubio@der.ucm.es. https://orcid.org/0000-0001-5074-0371

[3] Castells, M. (1998). The information age: economy, society and culture. Vol. III. End of millenium. Willey-Blackwell. p. 1.

alarma[4]. Mientras tratamos de averiguar los efectos que tiene sobre el comportamiento político, la posverdad va transformando el ecosistema democrático y su interacción social de manera considerable[5]. Por eso resulta imprescindible seleccionar momentos claves del debate político, como las campañas electorales, para tratar de aislar el problema y poder estudiarlo con detalle. En línea con lo señalado por De Vega: "Como momento decisivo en la vida democrática de cualquier país, las campañas electorales adquieren el valor de testimonio en el que aparecen reflejadas las grandezas y miserias de la democracia moderna"[6].

1. LA TECNOLOGÍA ELECTORAL Y SU USO EN CAMPAÑA

La campaña electoral es un periodo concreto dentro del proceso electoral en el que se persigue "una difusión masiva de información de coste nulo para el elector, en tiempo y en dinero"[7]. Este acto de comunicación responde a un doble fin: la búsqueda del voto partidista, "ponerse en contacto con el cuerpo electoral para atraer el máximo número de votos."[8], y la integración de la ciudadanía en la formación de la voluntad general mediante su intervención en los debates sobre el bien común. En ocasiones ambos pueden resultar incompatibles. Aunque la promoción del voto no debería hacerse a costa de la integración ciudadana, cada vez es más frecuente que sea así, cuando la movilización del afín y la desmovilización del no partidario "entran en competencia para obtener los sufragios de los ciudadanos"[9], superando la visión tradicional que concibe las campañas electorales como un enorme y simbólico diálogo entre electores y elegibles, entre representados y representantes. Ocurre, no obstante, que la revolución operada en los medios de comunicación determina que ese impresionante diálogo colectivo sufra una conmoción notable, en la medida en que acaba haciendo "sucumbir a los principios inspiradores de la conducta del homo sapiens ante los requerimientos y urgencias del homo videns"[10]. Como consecuencia de esta evolución, las campañas electorales han sido percibidas, y por tanto diseñadas normativamente, como periodos de alta intensidad en la utilización de técnicas de comunicación persuasiva y disuasiva. De ahí que, en el

[4] Rubio Núñez, R., y Vela, R. (2017). *Parlamento Abierto: El parlamento en el siglo XXI*. UOC Editorial. Pp. 13-31.

[5] Rubio Núñez, R. (2018). "Los efectos de la posverdad en la democracia". *Revista de Derecho Político*, n. 103, UNED.

[6] De Vega, P. (2017), "Democracia y Elecciones", en Obras escogidas, CEPC, Madrid, p. 775.

[7] López-Guerra, L. (1977). *Las campañas electorales en Occidente*. Barcelona: Ariel. p. 17.

[8] De Carreras, F. y Vallés, J.M., (1977) Las elecciones. Introducción a los sistemas electorales. Blume, Barcelona, p. 60.

[9] Arnaldo Alcubilla (2009). "El procedimiento electoral en leyes electorales autonómicas", en Gálvez Muñoz, L. (dir.), *El Derecho electoral de las Comunidades Autónomas. Revisión y Mejora*. Madrid: CEPC, p. 373.

[10] De Vega, P. (2017), "Democracia y Elecciones", en Obras escogidas, CEPC, Madrid, p 775.

proceso de acceso al poder instrumentalizado a través de las elecciones periódicas, observamos cómo incluso las reglas del juego han cambiado en favor de esta idea. La propaganda fagocita el debate público, todo apela a los sentimientos, a las emociones, al componente irracional de la política. Los tiempos en los que se elabora y distribuye la información se han reducido considerablemente. El espacio de las campañas se ha desplazado a las redes y han aparecido nuevos sujetos con capacidad de influencia en el proceso electoral, distintos de los tradicionales partidos y medios de comunicación.

Además, el aumento de la importancia de la tecnología en los procesos electorales redobla la importancia de este tipo de enfoques. Hay que tener en cuenta que la tecnología ha permitido extender el ejercicio del derecho al voto gracias al voto electrónico (Brasil), mejorar su transparencia y las posibilidades de control con la publicación online de todas las actas (Indonesia) o aumentar la eficacia del sistema y la confianza en el mismo, ofreciendo resultados en un tiempo reducido que acorta los momentos de incertidumbre (algo cada vez más frecuente en las elecciones de todo el mundo). También en las campañas electorales la tecnología se ha convertido en un elemento diferenciador. Es tal su protagonismo en estos procesos que, en los últimos tiempos, algunas de ellas han terminado por caracterizar informalmente las campañas presidenciales norteamericanas, pioneras en la incorporación de técnicas del marketing político. Así se habla de las elecciones de Meetup en 2004, de las redes sociales (MyBO) en 2008, de la microsegmentación en 2012, de Twitter y la publicidad en Facebook (impulsada por Cambridge Analytica) en 2016, de la desinformación en 2020 y de la IA en 2024.

Asistimos a una nueva etapa en la historia de las campañas electorales[11], en las que hasta ahora se distinguían tres momentos clave:

Las campañas premodernas, que podemos situar en el siglo XIX y el principio del siglo XX, se caracterizan por su naturaleza personal (P2P). La tecnología se reducía a una plataforma en la parte trasera de un tren y la necesaria para elaborar y distribuir prensa escrita, fundamentalmente local. Este tipo de campañas basadas en mítines y movilización personal, de tierra, premiaban las estructuras partidistas y diluían la figura de un líder al que la inmensa mayoría de los votantes no podían ver ni oír durante toda la campaña.

La irrupción de los medios de comunicación de masas, como la radio y la televisión, dieron paso a las campañas electorales modernas. Estas comenzarían en la década de los 20 del siglo XX y se prolongarían hasta los año 80 del mismo siglo, y estaban basadas en la difusión de información a través de medios de comunicación masivos (P2M). Las campañas modernas ofrecían más posibilidades de conocer y dar a conocer las propuestas políticas de los candidatos, dando visibilidad a

[11] Norris, P. The evolution of campaign communications. Anais do congresso Political Communications in the 21st Century, University of Otago, New Zealand, Janeiro de 2004. Disponible en: [https://www.academia.edu/2749582/The_evolution_of_election_campaigns_Eroding_political_engagement]. Consultado: 20.12.2023.

espacios de debate público, aunque propiciaron también un mayor personalismo, cierta dependencia de profesionales técnicos, y una mayor dependencia emocional del voto[12].

Por último, las campañas posmodernas, que van desde los años 80 hasta nuestros días, estarían caracterizadas por la irrupción sucesiva de distintas tecnologías informáticas que, entre otros efectos, introdujo elementos de persuasión basados en un mejor conocimiento de los públicos objetivos, sus lógicas y motivaciones, y una mayor capacidad técnica de hacerles llegar el mensaje (segmentación), así como la posibilidad de utilizar la tecnología como herramienta de información masiva y, sobre todo, de movilización.

Sin embargo, la irrupción de las técnicas de IA, estarían dando paso a una cuarta etapa, la de las campañas algorítmicas.

2. LA AMENAZA TECNOLÓGICA

Este protagonismo tecnológico en las campañas electorales viene acompañado, al mismo tiempo, de las denuncias en todo el mundo sobre la fragilidad del sistema electoral. "Esta fragilidad tiene una relación directa con la tecnología, y afecta a las distintas fases del proceso electoral: campaña electoral, votación y recuento"[13]. De esta manera se han multiplicado las amenazas de ataques tecnológicos que buscan alterar o colapsar el sistema de forma general o selectiva y la utilización fraudulenta de la tecnología que pone en riesgo principios básicos de la contienda como la libertad del voto o la equidad electoral. El sistema electoral, incluso cuando se apoya en un grupo amplio de personas e instituciones, depende de la tecnología en fases claves como la elaboración y distribución de los censos o la transmisión de los resultados y su puesta en común; una dependencia que puede ser aún mayor en lugares en los que es necesario solicitar la inscripción al censo o, evidentemente, en sistemas que han incorporado el voto electrónico. En este campo se han denunciado ataques a los censos de localizaciones específicas, que buscaban excluir a determinados votantes o retrasar el ejercicio del voto provocando aglomeraciones que disuadieran selectivamente del ejercicio al voto (Estados Unidos)[14], o amenazas al sistema de recuento hasta provocar el abandono del recuento electrónico, realizandose la votación en su

[12] Sartori, G. (1989) Homovidens. La sociedad teledirigida. Taurus.

[13] Burguera Ameave, L., y Rubio Núñez, R. (2015). "Información y propaganda. La comunicación política y electoral en la época del gobierno abierto", en Bel Mallén, J.I., y Corredoira Alfonso, L. (Dirs.), *Derecho de la información: el ejercicio del derecho a la información y su jurisprudencia*. Madrid: CEPC, pp. 291-318.

[14] Disponible en [https://www.brennancenter.org/our-work/policy-solutions/preparing-cyberattacks-and-technical-failures-guide-election-officials], consultado: 17.09.2024.

totalidad en papel, el escrutinio manual e incluso la comunicación de los resultados por vía telefónica en lugar de por ordenador (Países Bajos, 2017)[15].

El ataque a las infraestructuras tecnológicas también puede afectar a la campaña electoral, con el robo de información privada, los ataques de denegación de servicios (DoS) que sobrecargan el tráfico a páginas webs para interrumpir su funcionamiento normal o los hackeos a bases de datos. A esto se unen prácticas como la segmentación del votante y la correspondiente personalización de la información, pagada u orgánica, que se hace llegar a estos perfiles (práctica popularizada por la empresa Cambridge Analytica en campañas como la del referéndum sobre la permanencia del Reino Unido en la Unión Europea, celebrado en 2018); la interferencia de personas o grupos distintos de los partidos políticos, tanto desde dentro como desde el exterior del territorio en el que se celebran las elecciones, con la compra de publicidad o mediante acciones coordinadas de *astroturfing* (práctica denunciada, y demostrada, en las elecciones presidenciales norteamericanas de 2016 y 2020); la creación de perfiles falsos (*bots*) para crear corrientes de opinión favorables (como en el referéndum sobre el aborto en Irlanda de 2018); o el uso de plataformas de comunicación interpersonal para distribuir masivamente mensajes de desinformación (en la que destaca el uso de WhatsApp que hizo en la campaña presidencial brasileña Jair Bolsonaro en 2018[16]). Todas estas prácticas, tras irrumpir sorpresivamente en un proceso electoral, se han terminado extendiendo entre las fuerzas políticas, traspasando sus fronteras iniciales, y normalizando su uso, que se vuelve universal y transversal.

En resumen, actualmente las campañas electorales se han convertido en un proceso de interacción comunicativa que incrementa el número de emisores, amplia los espacios de campaña llegando a los canales de comunicación personal, reduce los tiempos de distribución de los mensajes, y los multiplica, sujetos a una fuerte carga emocional y manipulativa, gracias a las técnicas de microsegmentación[17]. Es difícil cuantificar el impacto de estas prácticas o discernir si realmente afectan al comportamiento electoral del votante; y resulta arriesgado afirmar sin ambages que logran alterar los resultados de unas elecciones. Sin embargo, no existen tantas dudas en señalar cómo estas técnicas de campaña, donde el acceso a la información está mediado por algoritmos, y se combinan técnicas de persuasión microsegmentadas y desinformación, suponen una amenaza para la democracia al atacar su raíz, que es la confianza.. Más aun, en el periodo electoral lo hace de una forma mucho más agresiva o dañina, por cuanto afecta al fundamento de la confianza en la democracia: el

[15] Disponible en {https://english.kiesraad.nl/latest-news/news/2017/06/13/evaluation-of-the-2017-elections-to-the-house-of-representatives-new-ballot-paper-model-and-electronic-counting}, consultado: 17.09.2024.

[16] Sánchez Muñoz, Ó. (2020). *La regulación de las campañas electorales en la era digital. Desinformación y microsegmentación en las redes sociales con fines electorales*. Madrid: CEPC.

[17] Burguera Ameave, L., y Rubio Núñez, R. (2015). "Información y propaganda. La comunicación política y electoral en la época del gobierno abierto", op. cit.

sistema de elección de los representantes, que es de donde obtienen su legitimidad los elegidos.

3. LA DIGITALIZACIÓN DE LA INFORMACIÓN (Y LA DESINFORMACIÓN) ELECTORAL

Como recordábamos hace años: "El contexto político condiciona y determina los conceptos de información y propaganda hasta situarlos en un espacio de significado continuo del que es difícil deslindar los límites. El motivo de esta difusa distinción obedece a la percepción generalizada de que la democracia descansa sobre la base de una comunicación persuasiva. Una comunicación que oculta la existencia de una intencionalidad por parte de aquel que transmite un mensaje o idea y que en el fondo tiene tras de sí unos objetivos conscientes, prefijados y específicos que buscan la captación de votos. En este sentido se ha entendido durante mucho tiempo propaganda y publicidad como sinónimos, de forma que la propaganda emplearía las técnicas tradicionales de la publicidad para promover contenidos «políticos», ideas y creencias."[18]. Esta asimilación entre ambos conceptos hace cada día más difícil diferenciar entre las distintas formas de campaña, por lo que se busca acudir a criterios objetivos como la existencia de un pago, más propia de la publicidad, que hoy resultan insuficientes como criterio diferenciador al existir otras formas de publicidad no convencionales que se apoyan en la generación de contenidos y su distribución "orgánica" sin necesidad de pagar a la plataforma por su distribución.

A esto se añade la digitalización de las campañas, que las dota de ciertas peculiaridades, aunque solo sea porque multiplica exponencialmente el volumen de información y de sus emisores, adoptando formatos poco tradicionales que afectan tanto al contenido como a sus formas de transmisión. Como señalaba Benedicto XVI en su mensaje con motivo de la XLV Jornadas de las Comunicaciones Sociales: "Las nuevas tecnologías no modifican sólo el modo de comunicar, sino la comunicación misma"[19]. La desinformación que amenaza los procesos electorales adquiere así carácter estructural, al desarrollarse en un nuevo escenario donde el poder de producción es sustituido por el poder de definición y donde la información es el instrumento clave para ello. Esta desinformación, cuando se realiza de manera profesional y cuenta con recursos humanos y materiales suficientes, se convierte en una amenaza para la estabilidad democrática. Su profesionalización provoca que no se limiten al periodo electoral, cuando se intensifican las acciones que necesitan de mucho tiempo

[18] Burguera Ameave, L., y Rubio Núñez, R. (2015). "Información y propaganda. La comunicación política y electoral en la época del gobierno abierto", op. cit.

[19] Benedicto XVI. (2011). "Mensaje del Santo Padre Benedicto XVI para la XLV Jornada Mundial de las Comunicaciones Sociales. Verdad, anuncio y autenticidad de vida en la era digital". Disponible en: https://www.vatican.va/content/benedict-xvi/es/messages/communications/documents/hf_ben-xvi_mes_20110124_45th-world-communications-day.html.

y trabajo de preparación previa, sino que se incorporan a la práctica habitual de partidos e instituciones. De esta manera la evidencia muestra cómo estas estructuras permanentes de desinformación —estatales o partidistas— han ido aumentando de manera progresiva en los últimos años[20].

Si, como se repite constantemente, la desinformación no es un fenómeno nuevo, el empleo de la tecnología dota esta práctica de nuevo contenido y a nueva velocidad, y nueva versión resulta imprescindible para buscar respuestas. De un lado, el exceso de información provoca inflación informativa, horizontalidad y la consiguiente pérdida de autoridad de los referentes informativos tradicionales. Se genera así un tipo de consumo informativo selectivo de «verdad a la carta» donde se pueden ignorar aquellos hechos que no coinciden con nuestro punto de vista, automatizando estos filtros informativos hasta olvidarnos de que existen, con el consiguiente peligro de confundir nuestra realidad con la realidad. A esto habría que añadir la reducción de los tiempos informativos y, con ellos, el debilitamiento de los procesos de verificación, elaboración y reflexión. Esto refuerza la pérdida de horizonte temporal de la política, convertida en un "presente omnipresente"[21] donde cada declaración, cada acto, parece empezar de cero, sin ningún condicionante en el pasado y sin ninguna obligación para el futuro. De otro lado, la hiperconexión[22] condiciona la distribución de una desinformación que se distribuye masivamente gracias a que los ciudadanos se encuentran hiperconectados, especialmente a través de canales de comunicación interpersonal como WhatsApp o Telegram. Esta hiperconexión, o hipersocialización, alimenta y facilita el deseo de mantener la coherencia de una cosmovisión con el grupo[23], lo que puede acabar condicionando las decisiones políticas de una forma todavía más poderosa que los propios sesgos personales.

---

[20] Bradshaw, S., y Howard, P. (2017). *Troops, trolls and troublemakers: a global inventory of organized social media manipulation*. Oxford: University of Oxford. Disponible en: [https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdfhttps://demtech.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf]; Bradshaw, S. Howard, P. N. (2018) Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation. Oxford Internet Institute: University of Oxford. Disponible en: [https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2018/07/ct2018.pdf]; Bradshaw, S. Howard, P. N. (2019) The Global Disinformation Order 2019. Global Inventory of Organised Social Media Manipulation. Oxford Internet Institute: University of Oxford. Disponible en: [https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf]; Bradshaw, S. Bailey, H. Howard, P. N. (2020) Industrialized Disinformation 2020 Global Inventory of Organized Social Media Manipulation. Oxford Internet Institute: University of Oxford. Disponible en: [https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf] consultados el 17.09.2024.

[21] Burguera Ameave, L., y Corbacho López, A. (2013). "El derecho al olvido de los políticos en las campañas electorales", en Corredoira, L., y Cotino Hueso, L. (eds.), *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*. Madrid: CEPC.

[22] Arriagada, E. (2023) Hiperconectados: Cómo comunicarse en el siglo XXI. Santiago de Chile: Forja.

[23] Kahneman, D., Sibony, O., Sunstein, C. (2021) Noise. Little, Brown & Company, Nueva York.

En el terreno electoral, los cambios descritos propician los siguientes efectos:

(i) La fragmentación es a la vez causa y consecuencia. Como consecuencia de esa verdad a la carta en la que cada uno construye, consciente o inconscientemente, su dieta informativa, lo que antes llamábamos la esfera pública —entendida como una especie de lugar imaginario donde se producía el diálogo social y político— se fragmenta, de tal manera que se sustituye por un conjunto de pequeños nichos sin relación, cuestionando el modelo de democracia deliberativa habermasiano, que en las últimas décadas se ha defendido como modelo ideal de democracia.

(ii) El aumento de posiciones extremas y la polarización —consecuencias directas de la fragmentación y del aislamiento— hace más difícil que se practique la costumbre de conocer y ponerse en el lugar del otro. En cambio, facilita que se silencia y expulse al que piensa de manera diferente, provocando una retroalimentación permanente: la competencia por la atención dentro de grupos homogéneos supone alzar el tono siempre un poco más que los que nos rodean, ya sea en el fondo o en la forma, lo que provoca que estos grupos cerrados acaben polarizándose de manera casi natural empujados por dinámicas de radicalización.

(iii) Como consecuencia lógica de todo lo anterior, se produce el incremento del componente espectacular de la política, convertido en el entorno ideal de la desinformación, que a su vez se acentúa en el periodo electoral y también amenaza a la democracia. Un espectáculo que aumenta el peso del emotivismo en la democracia[24] y, reforzado por el elemento temporal ya mencionado, fomenta la volatilidad de la política, con la consiguiente dificultad de establecer planes a medio o a largo plazo.

(iv) En el terreno cultural, las lógicas de deslegitimación fomentadas por la desinformación refuerzan posiciones populistas, que contraponen la supuesta voluntad del pueblo al resultado de las urnas y terminan en un intento de sustitución de la democracia representativa por un concepto de democracia directa sin contrapesos. Se trata de un tipo de participación política que premia el activismo y minusvalora al ciudadano pasivo; el propio ruido que generan las redes sociales acaba convirtiéndose en un elemento determinante a la hora de tomar decisiones.

(v) El proceso anterior crea las condiciones favorables para la manipulación del proceso electoral, la disminución de la confianza en el proceso y en el sistema democrático. Un malestar que alimenta la desafección, y podría conducir a la fatiga democrática e inducir la desvinculación progresiva de los ciudadanos de los procesos políticos, partidistas y electorales.

[24] Arias Maldonado, M. (2016). *Democracia Sentimental: política y emociones en el siglo XXI*. Madrid: Página Indómita.

4. USO DE LA IA EN LAS CAMPAÑAS ELECTORALES

En este contexto, la inteligencia artificial (IA), que está cobrando protagonismo creciente en áreas como la investigación científica o los negocios y ayudando a la sociedad a organizarse de manera más eficiente y a los poderes públicos a brindar un mejor servicio a sus ciudadanos, también está impactando intensamente en el comportamiento de organizaciones, partidos políticos, candidatos y activistas en el ámbito de las disputas simbólicas que caracterizan la política del siglo XXI.

En lo electoral, la irrupción de la IA ha dado lugar a una nueva fase en la evolución de las campañas electorales, las campañas algorítmicas, que amenaza con la progresiva deshumanización de las campañas electorales que, ya fuera a través de los contactos interpersonales directos, la intermediación de los medios de comunicación de masas o en la modalidad multiplataforma propia de la digitalización, siempre conservaron —a pesar de la transformación de los canales y las técnicas— su carácter humano.

No cabe mirar hacia otro lado, o promover su exclusión de la vida política. La IA se está consolidando como una herramienta que condiciona el ejercicio efectivo de los derechos políticos pasivos, ya que infrautilizar su potencial disolverá las posibilidades de éxito en las contiendas electorales. En un futuro muy próximo, las campañas que no utilicen estas técnicas, especialmente en las grandes circunscripciones, serán cada vez más caras y menos eficaces, ya que la comunicación generalista parece cada vez menos capaz de movilizar a los votantes. El uso de estas técnicas, como cualquier tecnología que irrumpe en campaña, generaría un efecto imitación, que provocaría en un breve espacio de tiempo su generalización y un riesgo de convertir la campaña en una guerra entre tecnologías, en la que triunfaría la más efectiva, lo que supondría en la práctica el fin de las campañas electorales tal y como las conocemos, pese a la aparente continuidad de las mismas, al mantenerse los elementos propios de un proceso electoral como discursos, anuncios, mensajes, votación y recuento.

Ya podemos encontrar, en la práctica, usos que, sin alterar esta lógica democrática, aumentan la capacidad de persuasión de partidos y candidatos. Se trata de usos que mejoran la capacidad de dar a conocer las propuestas, su llegada y su accesibilidad y promueven el diálogo. En este sentido, las técnicas de IA brindan oportunidades para una comprensión diferenciada de los escenarios, para el desarrollo de estrategias sofisticadas y para optimizar la comunicación entre los líderes políticos y la población, además de permitir aumentar las capacidades institucionales de los organismos electorales, por ejemplo, en el ámbito de la mejora de las relaciones con la sociedad, la organización electoral, la identificación de votantes, la actualización de registros o la lucha contra la desinformación, tanto en la detección de contenidos objetables, a través del monitoreo y la escucha social, como en la comunicación frente a esta, con la difusión de aclaraciones, utilizando el "contradiscurso" como "táctica de combate" contra el mal de la desinformación.

Pero si proyectamos hasta dentro de unos años las potencialidades de la IA, el escenario futuro genera cierta inquietud. Los sistemas de IA reconfiguran la esfera pública, que pasa a ser fragmentada, inducida, irreal y falsificada, disminuyendo su racionalidad y su naturaleza libre e informada. Resucitan deformaciones y desigualdades, afectando al modo en que la información circula y es accedida por el cuerpo social. El papel decisivo de los algoritmos opacos y sesgados de los sistemas de recomendación fagocita el núcleo de la agenda política, creando cámaras de eco que alimentan burbujas identitarias. Esto genera que se intensifique el sectarismo y la intolerancia ideológica y favorece la normalización de campañas negativas, discursos de odio. Así, se crea un piso fértil para la radicalización y los ataques de grupos que pretenden desestabilizar la sociedad, y se crean las condiciones perfectas para movimientos antidemocráticos que utilizan como pretexto fraudes inexistentes. Sin embargo, el riesgo más grave parece ser la erosión de la confianza: en la era de la IA, el consenso fiduciario se ve socavado por falacias de alto rendimiento, y el tejido social se deshilacha en un entorno de sospecha permanente. La desconfianza y la división se unen para elevar las hostilidades, el odio, la inseguridad y la polarización, revelando un mundo en el que la inestabilidad trata de imponerse como la nueva normalidad y envenenando el proyecto democrático, que está ligado a la condición del pluralismo.

El decisivo avance de la inteligencia artificial anuncia una nueva, inminente e inevitable transformación en la dinámica de los procesos electorales. El uso de la IA en los mismos se sitúa en un contexto general en el que hemos pasado de la visión utópica de poner en la tecnología todas las esperanzas de regeneración democrática (por su impulso a la transparencia, la participación y la rendición de cuentas) a una visión apocalíptica, según la cual es de la tecnología de dónde vienen todos los males que aquejan a una democracia, que estaría viviendo sus últimos días como consecuencia de la misma. En este contexto, los procesos electorales ocupan un lugar central en la legitimidad del sistema democrático, y el uso en los mismos de la IA, por su complejidad y opacidad, puede contribuir a esta reacción de rechazo.

Se inaugura, así una época de "elecciones de alto riesgo"[25] que afrontamos en ausencia de una regulación específica, eficaz y completa. El modelo emergente puede afectar a aspectos centrales de la legitimidad democrática. Las elecciones integras y legítimas sólo prosperan cuando prevalecen los valores democráticos, lo que exige —de la sociedad en su conjunto— una mayor atención a las externalidades de la normalización del uso de estos medios tecnológicos desde una perspectiva social.

De ahí que el uso de la IA en los actuales procesos electorales esté suscitando distintos temores[26]. Así se ha demostrado en elecciones, finalizadas o en curso, en países

[25] Alvim, F.F., Rubio, R. y Monteiro, V. A. (2024). Inteligência Artificial e eleições de alto risco. Ciberpatologías e ameaças sistémicas da nova comunicaçao política. Rio de Janeiro: Lumen Juris.

[26] Consejo de Europa. (2022). "Artificial Intelligence and Electoral Integrity". Concept Paper. Disponible en: https://www.coe.int/en/web/electoral-management-bodies-conference/concept-paper-2022; Foro Económico Mundial. (2024). *The Global Risks Report 2024: Insight Report, 19th Edition*. Disponible en: https://www.weforum.org/reports/global-risks-report-2024/.

como Eslovaquia donde el uso de *deepfakes* irrumpió a pocas horas de la celebración de la primera vuelta de las elecciones presidenciales de 2023, con la filtración de un *deepfake* donde el líder del partido progresista decía haber comprado votos a una minoría étnica[27]; Argentina donde se utilizó IA en la elaboración de carteles electorales en la campaña de Sergio Massa[28]; México donde se cruzaron las acusaciones sobre si determinadas declaraciones e imágenes se habían realizado con IA o habían ocurrido en realidad[29]; Estados Unidos donde aparecieron *deepfakes* de voz desanimando a los demócratas de votar en las primarias[30] o imágenes que mostraban a Donald Trump junto a votantes negros, y que se demostraron generadas por IA en un esfuerzo por atraer ese segmento de votantes[31]; en India se simuló un mensaje de una estrella de Bollywood en contra del BJP indio, criticando al primer ministro Modi[32]; en Pakistán se distribuyó también un video generado por IA de Trump prometiendo su apoyo al ex-primer ministro Imran Khan[33], en Sudáfrica simularon al mundialmente conocido Eminem apoyando al partido opositor EFF[34]; en Indonesia, también se distribuyó un audio falso fingiendo la discusión entre dos líderes de un mismo partido político[35]. Por si existía alguna duda de que la automatización de algunos procesos, a través de los algoritmos, y especialmente a través de sistemas de inteligencia artificial en la maquinaria electoral está transformando la dinámica de las elecciones.

El primer efecto, y más evidente, es el de la desinformación y la manipulación de la realidad. La IA facilita la difusión estratégica y coordinada de desinformación, a través de estrategias de infoxicación, que buscan colapsar la agenda informativa, la creación de fuentes informativas ad hoc o la puesta en circulación de pseudomedios o la creación y gestión de perfiles sociales automatizados que participan en el debate

---

[27] Disponible en: [Trolls in Slovakian Election Tap AI Deepfakes to Spread Disinfo], consultado el: 4.5.2024

[28] DURÃES, Ueslei. 'Novo estágio das fake news: deepfake vira arma de campanha na Argentina'. **UOL**, 18 de noviembre de 2023. Disponible en: [https://noticias.uol.com.br/internacional/ultimas-noticias/2023/11/18/novo-estagio-das-fake-news-deepfake-vira-arma-de-campanha-na-argentina.htm]. Consultado: 26.04.2024.

[29] Disponible en: [Un polémico audio con la voz de Martí Batres echa más leña al fuego en la carrera por la candidatura de Ciudad de México], consultado el: 4.5.2024.

[30] Disponible en: [New Hampshire opens criminal probe into AI calls impersonating Biden - The Washington Post], consultado el: 4.5.2024

[31] Disponible en: [Eleição nos EUA: apoiadores de Trump usam fotos falsas pra atrair eleitores negros - BBC News Brasil], consultado el: 4.5.2024.

[32] Disponible en: [Aamir Khan & Ranveer Singh criticising PM Modi! Think again, that's deepfake drama - The Economic Times], consultado el: 4.5.2024

[33] Disponible en: [Deepfake Video Of Donald Trump Promising Support To Ex-Pak PM Imran Khan Goes Viral Ahead of US Polls], consultado el: 4.5.2024

[34] Disponible en: [Will the real Slim Shady please stand up? Eminem video endorsing South African opposition party EFF and bashing the ruling ANC is a deepfake - Africa Check], consultado el: 4.5.2024

[35] Disponible en: [Anies Buka Suara soal Hoaks Rekaman Dimarahi Surya Paloh], consultado el: 4.5.2024

público y buscan reforzar determinadas ideas o atacar otras con técnicas como el *astroturfing*. También permite alterar el contenido de la información, e incluso generar contenido de cero, tergiversando la realidad y ofreciendo una imagen falsa de la misma, con la generación a través de Inteligencia Artificial Generativa (IAG) de *cheapfakes* (*shallowfakes*) o *deepfakes*, de audio y vídeo. De esta forma, se han incorporado a las campañas distintos mecanismos que, impulsados por IA, están aumentando el alcance y la eficiencia de la propaganda política, por el uso industrial de estas herramientas en la producción y distribución de contenidos nocivos o desinformativos, que inundan las redes y los canales de mensajería y alcanzan a los medios de comunicación que los recogen con mejor o peor intención, y que, además, pueden ser impulsados con el uso de envíos masivos y la creación de cuentas sospechosas, en muchos casos resultado de la programación selectiva (utilizando también IA) de diversos tipos de bots.

El segundo afecta a la libertad del voto (su autodeterminación ajena a presiones externas), en lo que podríamos denominar el "hackeo cognitivo". Estas nuevas técnicas de *big data* permiten captar datos del comportamiento de los votantes y procesarlos a través de distintos algoritmos que favorecen la adaptación automática de los mensajes para alterar artificialmente los grandes debates públicos, así como para influir negativamente en el mercado de la información y en el clima de las relaciones sociales, dañando la capacidad colectiva de comprensión de la realidad mediante técnicas de persuasión impensables en el pasado; aplican técnicas de microsegmentación psicográfica, elaborando perfiles en función, no sólo de datos sociológicos sino de datos extraídos del comportamiento individual, tanto en el mundo físico como en el digital, y la construcción de una estrategia comunicativa personalizada, adaptada a las creencias y circunstancias de pequeños grupos de votantes, o incluso de cada uno de ellos, construyendo para cada uno una realidad "a la carta" que no renuncia a utilizar engaños a medida. Estas técnicas se van perfeccionando gracias a la IA de manera circular, y al aplicarse van mejorando su conocimiento del individuo y su eficacia de manera progresiva, permitiendo a las plataformas sociales un profundo conocimiento incluso del subconsciente del individuo que permite influir en el comportamiento de las personas, a través de la explotación de debilidades, creencias y prejuicios, estableciendo conexiones de baja racionalidad y con una alta estimulación del aparato emocional (especialmente las emociones negativas como el miedo o el temor a la perdida), que en el ámbito electoral pueden condicionar la autonomía del voto.

El tercer efecto del uso de la IA en campaña es la fragmentación y la polarización, fruto del predominio de la comunicación emocional construida sobre el hecho de que "las falsas narrativas a menudo dependen de cómo se siente la gente sobre el tema, más que de lo que piensan sobre el asunto en cuestión"[36] y la consiguiente crisis de

[36] Bowman, N.D., y Cohen, E. (2020). "Mental Shortcuts, Emotion and Social Rewards", en Zimdars, M., y Mcleod, K., *Fake news: understanding media and misinformation in the Digital Age*. Cambridge: The MIT Press, p. 225.

confianza que abre la puerta a la lógica de la anti política. La "abierta hostilidad a la realidad verificable"[37], el "desprecio por los hechos, la sustitución de la razón por la emoción y la corrosión del lenguaje están disminuyendo el valor de la verdad", inflando una "polarización tóxica" e inoculando la intolerancia como un "virus" en el sistema político[38]. La IA, en combinación con otras tecnologías digitales, perfila el marco general de ideas y opiniones que llegarán a cada usuario, diseñando así la ventana a través de la cual los internautas contemplan el mundo. Dado que organizan todo lo que se verá, leerá u oirá, los algoritmos de la red contribuyen al auge de un mundo fragmentado. Estos espacios públicos fragmentados, también por influjo de los algoritmos, tienden al aislamiento y favorecen la polarización, incorporando al debate público teorías conspirativas[39], informaciones simplificadoras, provocadoras y poco constructivas, hasta el punto de asumir "identidades agresivas"[40], que a través de manifestaciones digitales de odio e intolerancia[41] devalúan la esfera pública, deslegitiman las instituciones democráticas, y alteran "los protocolos cívicos (con sus reglas de lo que se puede decir)"[42], rebajando la calidad de los procesos electorales. Todas estas dinámicas son inicialmente favorecidas, posteriormente amplificadas y finalmente promovidas activamente por el uso de técnicas de IA y fomentan la fragmentación, la polarización, la desestabilización y la instigación del conflicto, a través de la promoción de contenidos polarizadores, radicales o extremistas.

El cuarto efecto sería el acoso, la discriminación y la violencia política. Del mismo modo que conectan a personas que se conocen y se caen bien, o que comparten creencias y gustos similares, las redes también pueden ser un campo de batalla donde se enfrenten individuos y grupos que sienten y piensan de forma diferente, ya sea sobre cuestiones menores y, en principio, triviales, o sobre aspectos sensibles y muy relevantes. En este contexto, al igual que las comunidades digitales albergan usuarios comprensivos, tolerantes y comprensivos con la diferencia, las redes sociales, como consecuencia de su propia arquitectura que favorece las cámaras de eco y una cultura política basada en la moralización del debate político y la consiguiente réplica de

[37] Snyder, T. (2017). *Sobre a tirania. Vinte lições do século XX para o presente*. São Paulo: Companhia das Letras. p. 64.

[38] KAKUTANI, Michiko. A morte da verdade: Notas sobre a mentira na era Trump. Rio de Janeiro: Intrínseca, 2018. pp. 10-27.

[39] Salinas Olarte, M. (2023). "Teorías de la conspiración: un análisis socio-político", en Figueruelo Burrieza, A. (dir.), y Martín Guardado, S. (coord.), *Desinformación, odio y polarización*. Cizur Menor: Aranzadi, p. 338.

[40] Lassalle, J.M. (2021). *Liberalismo herido. Reivindicación de la libertad frente a la nostalgia del autoritarismo*. Barcelona: Arpa & Alfil. p. 185.

[41] Ramonet, I. (2022). *La era del conspiracionismo. Trump, el culto a la mentira y el asalto al Capitolio*. Buenos Aires: Siglo XXI. P. 163.

[42] Kiffer, A., Giorgi, G. Ódios políticos e política do ódio. Lutas, gestos e escritas do presente. Bazar do Tempo, Rio de Janeiro, 2019, p. 16.

comportamientos agresivos que tiene "efectos miméticos" en la base social[43], albergan hordas de individuos intolerantes, provocadores e incivilizados, aficionados a prácticas antidemocráticas y antisociales, expresadas en diferentes formas de discriminación, acoso y violencia política. Estas dinámicas, que podemos encuadrar en el discurso de odio, pueden explotarse con fines políticos de manera sistemática gracias a la propia IA, que, como consecuencia de sus sesgos y sus amplias posibilidades para coordinar este tipo de ataques (involucrando a *trolls* artificiales), amplifica el acoso a candidatos de grupos minoritarios y socialmente vulnerables. También se están utilizando otras técnicas de IA, como los *deepfakes*, como instrumentos de chantaje y acoso, que buscan la exclusión de determinados tipos de candidaturas.

El quinto tiene que ver con la ruptura de la equidad comunicativa. El peso que la IA está adquiriendo como instrumento de las campañas electorales puede hacer que su utilización sea un factor condicionante de los resultados. De ahí que, aunque no resulta razonable obligar a todos los actores políticos a utilizar la misma tecnología, sí resulta necesario que estas tecnologías estén por igual a disposición de todos los contendientes. Las plataformas, por su diseño, condicionan el acceso a la información. La IA, en combinación con otras tecnologías digitales, perfila el marco general de ideas y opiniones que llegarán a cada usuario, diseñando así la ventana a través de la cual los internautas contemplan el mundo, actuando como "agentes que, debido a su centralidad, ejercen todas las formas de control de la información en la red que crean, como la selección, el encuadre, el momento, la repetición, la retención, entre otras".

De esta manera, los algoritmos pueden "empujar a los votantes" hacia una corriente política concreta, tanto a través de anuncios personalizados[44] como de influencias sutiles que afectan a la formación de creencias, al desarrollo de la conciencia y a la consolidación de sus ideas y decisiones. En términos electorales, la "jerarquía discriminatoria de visibilidad"[45] genera procesos de exclusión y censura por defecto[46], y, por tanto, produce asimetrías en el equilibrio de oportunidades, ya que pone a los competidores directos en ventaja o desventaja, dependiendo de cómo se comporten los "espíritus invisibles de la codificación". A esto habría que añadir los efectos de la moderación de contenidos en las redes sociales, desarrollada mayoritariamente a través de sistemas que utilizan la IA para eliminar contenidos o reducir su visibilidad,

[43] Alvim, F.F., Zilio, R.L., y Carvalho, V.O. (2023). *Guerras cognitivas na arena eleitoral: o controle judicial da desinformação*. Rio de Janeiro: Lumen Juris. p. 454.

[44] Niyazov, S. (2019). "The Real AI Threat to Democracy". *Towards Data Science*. Disponible en: https://towardsdatascience.com/democracys-unsettling-future-in-the-age-of-ai-c47b1096746e.

[45] Shoai, A., y López Molina, A. (2023). "Polarización e inteligencia artificial: una sistematización del conocimiento disponible", en Vázquez-Barrio, T., y Salazar García, I. (eds.), *Inteligencia artificial, periodismo y democracia*. Valencia: Tirant lo Blanch, p. 255.

[46] Kissinger, H.A., Schmidt, E., y Huttenlocher, D. (2023). *La era de la Inteligencia Artificial y nuestro futuro humano*. Madrid: Anaya Multimedia. p. 97; Metaxas, P. T. (2020) "Technology, propaganda and the limits of human intellect". En: Zimdars, M., Mcleod, K. Fake news: understanding media and misinformation in the Digital Age. The MIT Press, Cambridge, p. 247.

e incluso para cancelar cuentas, grupos y canales, lo que vuelve prioritario mantener un equilibrio imparcial y neutral en el tratamiento y la moderación del contenido en las redes sociales, sin verse influenciado por inclinaciones políticas o partidistas.

El sexto tiene que ver con la simplificación de los mensajes políticos, ya que para adaptarse a los nuevos formatos utilizados durante las campañas y como parte de la interacción social de los usuarios, ya no existe un espacio para los grandes debates sobre las políticas públicas, y ahora se reducen al intercambio de slogans, en formatos atractivos y virales, para que tengan un eco entre los votantes.

Como consecuencia de todo lo anterior cobra especial relevancia el séptimo efecto del uso de la IA en campañas electorales, la ausencia de controles. La arquitectura de las redes se apoya en la economía, la ubicuidad, la facilidad de acceso y, sobre todo, el anonimato y esto facilita acciones tecnológicas indetectables o imperceptibles[47], ya sea en la dimensión de la manipulación de datos obtenidos ilícitamente, la construcción de *deepfakes* o la distribución robotizada de contenidos desinformativos a distintos niveles, que pueden comprometer los procesos electorales y cuyos autores gozan de refugio seguro[48].

La IA también desempeña un papel en estas cuestiones, ya que posibilita los ciberataques a distancia, y proporciona soluciones que socavan el sistema de rendición de cuentas al añadir varias capas de anonimato e impunidad, además de facilitar formas ocultas e imperceptibles de manipular los algoritmos de selección y sugerencia de contenidos (reinventando las estrategias de optimazación de los motores de búsqueda (SEO) o las prácticas de *clickbait*), alterando el régimen de suministro de información.

Asimismo, durante los procesos, las plataformas tecnológicas adoptan un número casi infinito de decisiones automatizadas relacionadas con contenido electoral. La naturaleza transnacional de las plataformas en red expone la protección democrática a algunos "fallos del sistema"[49], y la concepción anárquica de la ciberesfera, entendida como la esfera pública parcialmente digitalizada[50], exige el descubrimiento de fórmulas capaces de proteger el régimen de libertades, tanto dentro como fuera del

[47] Tasioulas, J. (2019). "First step towards and Ethics of robots and Artificial Intelligence". *Journal of Practical Ethics*, 7(1), p. 87

[48] Caiani, M., y Susánsky, P. (2021). "Radical-right political activism on the web and the challenge for European democracy. A perspective from Eastern and Central Europe", en Giusti, S., y Piras, E. (eds.), *Democracy and Fake News. Information Manipulation and Post-Truth Politics*. New York: Routledge, p. 175.

[49] Moore, M. (2022). *Democracia hackeada: como a tecnologia desestabiliza os governos mundiais*. São Paulo: Editora Hábito. p. 149.

[50] Olmeda Gómez, J. (2016) La digitalización de la opinión pública: ¿la ciberesfera como transformación estructural del espacio público?, Ciencia y política, una aventura vital. Libro homenaje a Ramón Cotarelo. Tirant lo Blanch, (pp.767-790).

ámbito electoral. De ahí la necesidad de reforzar la gobernanza algorítmica para la protección de la integridad de las consultas electorales en la era digital[51].

En este punto nos encontramos con la dificultad que tienen las instituciones públicas, especialmente los organismos electorales, de ofrecer una respuesta eficaz ante este nuevo escenario. Sus limitaciones técnicas, y la imposibilidad de hacer cumplir sus disposiciones en un espacio virtual, que se resiste a someterse a las legislaciones nacionales, provocan una dependencia tecnológica de las grandes plataformas en las que, ante la imposibilidad material de ofrecer soluciones, parecen poner su esperanza y su confianza. Esto supone una suerte de privatización de una parte del proceso de justicia electoral, que muchas veces se justifica por la ausencia de alternativas, pero que tiene graves consecuencias para los derechos electorales y la seguridad jurídica.

En resumen, el conjunto de cambios provocados por la generalización del uso de técnicas de IA en campaña, además de cambiar el entorno informativo, puede afectar directamente a la "arquitectura de decisión" del votante, propiciando una opinión cada vez más personalizada basada en segmentación y microsegmentación a gran escala; alterando la realidad, a través de la generación de contenido con IAG que desdibuja la distinción entre no ficción y ficción, y permiten formas más sofisticadas de engaño y manipulación, especialmente con el uso de *deepfakes*; y la difusión y redifusión de éstos, a través de mecanismos automatizados.

5. PRIMERAS RESPUESTAS

A pesar de que prácticas como la desinformación o la segmentación vienen amenazando la democracia incluso antes de la generalización de las nuevas herramientas de IA, lo cierto es que esta lleva el problema a una nueva dimensión. El uso de la IA en las campañas electorales supone un cambio importante en la forma de las mismas que afecta a su lógica democrática. Así lo señaló, Sam Altman, director ejecutivo de OpenAI, en su comparecencia ante el Senado de los Estados Unidos en mayo de 2023 cuando preguntado si pensaba que se podían utilizar los modelos de lenguaje basados en IA, como ChatGPT, para hacer que los votantes se comportaran de determinada manera, mostró su preocupación de que estos mecanismos puedan ser utilizados para persuadir, involucrar y manipular en relaciones personales con los votantes.

Este temor no responde a sus efectos en el momento actual, cuando los usos han sido puntuales y sus efectos visibles se han reducido al impacto de la creación y distribución de *deepfakes* horas antes de las elecciones que han logrado introducir la duda en el momento de la votación. Sin embargo, su uso se está generalizando y puede alterar el escenario en el que se desenvuelven las campañas en el medio plazo. Como consecuencia de la combinación de ambas, las empresas relacionadas con la

[51] Kofi Annan Foundation (2020). Protecting electoral integrity in the Digital Age. Koffi Annan Foundation, Geneve. p. 40.

IA han comenzado, individualmente o en grupo, a anunciar medidas destinadas a reducir este impacto.

5.1. **Autoregulación**

En este sentido, Meta[52] se ha comprometido a etiquetar las imágenes creadas con IA en todas sus plataformas, además ha declarado que prohibirá que las campañas políticas utilicen sus nuevos productos de publicidad generados por IA y requerirá que los anunciantes políticos revelen cuando utilicen herramientas de IA para modificar o crear anuncios en Facebook e Instagram. Su *Oversight Board*[53], organismo creado por la propia compañía para revisar las decisiones de Meta sobre moderación de contenido, en un documento frecuente de advertencias sobre el papel de la plataforma social en los procesos electorales señala la necesidad de establecer estándares claros para el contenido generado por IAG y *fakes (deep o cheap)*[54].

Google por su parte, además de etiquetar este tipo de contenidos en YouTube[55], ha restringido, desde comienzos de 2024, las respuestas relacionadas con las elecciones en su *chatbot* Gemini, ofreciendo como respuesta "Todavía estoy aprendiendo a contestar esta cuestión. Mientras, puedes consultar Google Search", restringiendo también la experiencia de búsqueda generativa relacionada con las elecciones.

Por último, OpenAI[56], creadora de ChatGPT y DALL·E, se compromete a prevenir el abuso, fomentar la transparencia y asegurar la integridad de las elecciones en todo el mundo. Tratando de anticiparse y prevenir el mal uso potencial de sus herramientas, especialmente en el contexto electoral. Para lograrlo ha puesto en marcha una serie de medidas para detectar y abordar el abuso, como identificar contenido generado por IA y prevenir la creación de *chatbots* que imitan a candidatos. Con esa intención, se introducirá un sistema de credenciales y marca de agua digital de la Coalición para la Proveniencia y Autenticidad del Contenido (C2PA) para identificar imágenes generadas por IA y, han anunciado el lanzamiento de un clasificador de procedencia para detectar imágenes generadas por DALL-E, incluso si han sido modificadas. Además, se implementará una función de "reporte" para usuarios, permitiéndoles señalar posibles violaciones en el uso de GPTs personalizados.

---

[52] Disponible en: [https://about.fb.com/news/2024/02/labeling-ai-generated-images-on-facebook-instagram-and-threads/], consultado el: 4.5.2024.

[53] Disponible en: [https://www.oversightboard.com/wp-content/uploads/2024/04/Oversight-Board-Elections-Paper-May-2024FINAL.pdf], consultado el: 4.5.2024.

[54] Disponible en: https://www.oversightboard.com/wp-content/uploads/2024/04/Oversight-Board-Elections-Paper-May-2024FINAL.pdf, consultado el: 4.5.2024.

[55] Disponible en: [https://www.npr.org/2023/11/14/1212986395/youtube-will-label-ai-generated-videos-that-look-real], consultado el: 4.5.2024.

[56] Disponible en: [https://openai.com/blog/how-openai-is-approaching-2024-worldwide-elections], consultado el: 4.5.2024.

Además de estas iniciativas particulares se ha lanzado una iniciativa conjunta en la que participan distintas empresas tecnológicas, el Acuerdo Tecnológico para Combatir el Uso Engañoso de la Inteligencia Artificial en las Elecciones[57]. Este incluye una serie de acciones y compromisos para neutralizar la difusión de contenidos producidos con sistemas de IA que puedan "comprometer la integridad de los procesos electorales". Materiales como imágenes, audio y vídeo generados con herramientas basadas en IA "que falsifican o alteran de forma engañosa la apariencia, la voz o las acciones de candidatos políticos, funcionarios electorales y otras partes interesadas". Los compromisos son:

1. Desarrollar y aplicar tecnología para mitigar los riesgos relacionados con contenidos electorales engañosos creados con sistemas de IA, incluidos los de código abierto.
2. Evaluar los modelos de IA en el ámbito del presente acuerdo para comprender los riesgos que pueden plantear en relación con la producción de contenidos electorales engañosos.
3. Controlar y detectar la distribución de tales materiales en sus plataformas.
4. Tomar medidas para tratar adecuadamente la información engañosa distribuida en sus servicios (etiquetado).
5. Fomentar la adaptación entre los sectores sensibles a los contenidos electorales engañosos.
6. Proporcionar al público información que haga transparentes las medidas de mitigación.
7. Colaborar con organizaciones académicas y de la sociedad civil para desarrollar planes de seguimiento.
8. Apoyar los esfuerzos para promover la concienciación pública, la alfabetización mediática y la resiliencia en toda la sociedad.

Sin embargo, en todos los casos, los principios y compromisos son genéricos y no contemplan explícitamente, por ejemplo, la prohibición o eliminación de las *deepfakes*. Tampoco incluyen detalles sobre cómo se aplicarán las resoluciones, ni siquiera un calendario de actuación.

5.2. Algunas propuestas internacionales

Por otro lado, el "informe sobre la Gobernanza de la IA en beneficio de la humanidad" se centra en la necesidad establecer un marco global de gobernanza para estos sistemas. El informe, elaborado por el Órgano Asesor de Alto Nivel sobre IA,

[57] Anunciado en febrero de 2024, el acuerdo en cuestión fue firmado por Adobe, Amazon, Anthropic, ARM, ElevenLabs, Google, IBM, Inflection AI, LinkedIn, McAfee, Meta, Microsoft, Nota, OpenAI, Snap, Stability AI, TikTok, TrendMicro, TruePic y X. Se puede acceder a su texto completo en la siguiente dirección: [https://www.aielectionsaccord.com/].

también alude expresamente al riesgo de "el aumento de la creación y difusión de desinformación". El documento apunta a la dificultad de regular la IA bajo marcos normativos tradicionales y las lagunas en la gobernanza global de estas técnicas, con los consiguientes problemas de coordinación, representación e implementación efectiva, cuando 118 países no están participando en ninguna iniciativa de gobernanza de la IA. Por lo que plantea la creación de un nuevo contrato social para la IA, una gobernanza integral, inclusiva y colaborativa que regule la IA a nivel global, que garantice que esta tecnología se despliegue en beneficio de toda la humanidad, sin dejar a nadie atrás.

También la OCDE ha elaborado una recomendación sobre Inteligencia Artificial, aprobada en 2019 y actualizada en 2024, que en su apartado sobre el respeto a los derechos humanos y valores democráticos, incluye como riesgos la información engañosa y la desinformación amplificada por la IA. La recomendación destaca la necesidad de hacer frente a estas amenazas "respetando al mismo tiempo la libertad de expresión y otros derechos y libertades protegidos por el Derecho internacional aplicable", como el derecho de acceso a la información. Esto significa que, si bien es necesario tomar medidas para limitar el uso malintencionado de la IA en la difusión de información engañosa, estas acciones deben ser proporcionadas y no deben inhibir el derecho de las personas a compartir opiniones y expresarse libremente. En este tema se recomienda que los actores de la IA pongan *"en marcha mecanismos y garantías, como la capacidad de intervención y supervisión humana, lo que incluye abordar riesgos derivados de usos distintos del fin perseguido, usos indebidos intencionados o usos indebidos no intencionados, de forma apropiada al contexto y coherente con el estado actual de la tecnología".*

Para abordar la desinformación, así como otra serie de riesgos sociales del uso de las técnicas de IA, la recomendación apunta a la cooperación entre gobiernos, empresas tecnológicas y otras partes interesadas. Esto implica compartir mejores prácticas, colaborar en la creación de normas internacionales que regulen el uso de IA para generar y difundir información, y desarrollar marcos legales adecuados para abordar el problema.

Además, la recomendación anima a los gobiernos a promover la alfabetización digital lo que repercutirá en que estas sean más conscientes de la existencia de la desinformación generada por IA, y puedan detectar mejor el contenido engañoso. Además, se habla de apoyar la creación de herramientas tecnológicas que ayuden a detectar y eliminar automáticamente la información falsa o manipulada, mientras se respetan los derechos fundamentales.

Entre las propuestas destaca, a efectos de nuestro estudio, las de Transparencia y explicabilidad, que apunta a los actores de la IA, que deben proporcionar información suficiente para que las partes afectadas puedan comprender cómo funcionan los sistemas de IA y cómo les afectan en sus interacciones concretas, y estén en condiciones, cuando se vean afectados negativamente, de cuestionar sus resultados. Esta transparencia incluiría, según la recomendación, *"información transparente y comprensible sobre*

las fuentes de datos/entradas, los factores, los procesos y/o el razonamiento que subyace a las predicciones, contenidos, recomendaciones y decisiones" lo que puede ayudar a los afectados por un sistema de IA comprender los resultados.

También resulta interesante para los procesos electorales la insistencia en la solidez y seguridad que indica que los sistemas de IA deben ser robustos, seguros y estar protegidos y que debe existir la capacidad de corregir o desmantelar sistemas si amenazan con causar daños. Además, cabe destacar el señalamiento a la responsabilidad de los actores involucrados sobre el respeto a los principios mencionados, con mecanismos como garantizar la trazabilidad y *"aplicar de forma permanente un enfoque sistemático de la gestión de riesgos a cada fase del ciclo de vida de los sistemas de IA".*

Por último, podemos aplicar a la desinformación el principio de mitigación del daño potencial, que supone que al detectar que un sistema de IA ha sido utilizado para propagar desinformación, los actores de la IA deben tener la capacidad de corregir o desmantelar esos sistemas. Esto, en nuestro ámbito, podría suponer eliminar contenido generado de manera maliciosa, ajustar los algoritmos para evitar futuros errores, o crear sistemas más robustos que no se presten fácilmente al abuso.

5.3. Respuesta legislativa

Todos estos problemas, originados por la manipulación de la información, se han vuelto sistémicos y necesitan ser abordados reconociendo el papel de los actores implicados y sus responsabilidades en el mantenimiento de los derechos de los votantes y de la propia democracia. La IA, plantea retos técnicos y sociales que, a su vez, exigen la adopción de un marco regulatorio por parte de las autoridades legislativas, administrativas y jurisdiccionales, para la protección de los procesos electorales. La "especial protección" del microsistema de la integridad electoral frente a las nuevas patologías que presenciamos en la era de las elecciones algorítmicas, en un contexto en el que las disputas políticas están impulsadas por los datos y en el que las plataformas sociales se afirman simultáneamente como "instituciones clave" de una "nueva plaza pública" y como los nuevos controladores de los procesos comunicativos que pueden llevar a los votantes a cambiar de opinión de forma casi inconsciente actuando como verdaderas "armas" de persuasión colectiva.

La Unión Europea ha sido pionera a la hora de blindar estos procesos electorales frente al uso fraudulento de la tecnología. Al existente Reglamento general de protección de datos (RGPD), que afecta al "tratamiento de datos personales en el contexto de unas elecciones" y establece una serie de previsiones y limitaciones como el consentimiento explícito, el tratamiento de datos para cumplir una obligación legal o de interés público, etc. incluidas las obligaciones de los responsables del tratamiento de datos. Entre estas obligaciones se encuentra la de los actores políticos de "informar a las personas sobre el tratamiento de sus datos y muy especialmente sobre la identidad del responsable, los fines del tratamiento, fuentes de los datos,

destinatarios, etc. Obsérvese que en el contexto de unas elecciones la serie de datos recogidos y tratados pertenecen muchos de ellos a la categoría de sensibles, por lo que tanto los encargados como los responsables del tratamiento tienen que aplicar medidas adecuadas para garantizar el nivel de seguridad que se exige en proporción con los riesgos que entrañan."[58].

También se aplica la Directiva 2022/2555 del Parlamento europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, que al recalcar que las entidades pertenecientes al sector de las infraestructuras digitales se basan esencialmente en sistemas de redes y de información, que subraya la necesidad de la seguridad física de dichos sistemas como parte de sus medidas para la gestión de los riesgos de ciberseguridad ya que, como hemos visto, su utilización en periodo electoral puede atacar la integridad del proceso y provocar desconfianza en el funcionamiento del mismo.

Además, la reciente aprobación del reglamento sobre IA también afecta a las campañas electorales. Este reglamento, "establece un modelo de regulación basada en la responsabilidad proactiva de los distintos actores que participan en el desarrollo, implementación y comercialización de las herramientas basadas en IA, y lo hace con un enfoque que parte de la delimitación de niveles de riesgo en función de la tecnología empleada y de sus usos posibles" [59].

Para hacer frente a estos riesgos específicos, el Reglamento Europeo de Inteligencia Artificial prevé cuatro modalidades:

- Riesgos mínimos o inexistentes: la mayoría de los sistemas de IA con riesgos insignificantes pueden seguir funcionando sin regulación;
- Riesgos limitados: los sistemas de IA con riesgos aceptables están sujetos a ligeras obligaciones de transparencia para que los usuarios puedan tomar decisiones con conocimiento de causa;
- Riesgos elevados: se autorizará un amplio espectro de sistemas de IA de alto riesgo, pero con requisitos y obligaciones estrictos para acceder al mercado de la UE[60] ;
- Riesgos inaceptables: se prohibirán, con limitadas excepciones, los sistemas que contengan riesgos considerados inaceptables, como la manipulación cognitiva, la vigilancia policial predictiva, el reconocimiento de emociones

[58] García Mahamut, R. (2023) Elecciones, protección de datos y transparencia en la publicidad política: la apuesta normativa de la UE y sus efectos en el ordenamiento español. Revista Española de la Transparencia, Núm. 17. Número Extraordinario, p. 75-105.

[59] Simón Castellano, P. (2023) La evaluación de impacto algorítmico em los derechos fundamentales. Navarra: Aranzadi. p. 26.

[60] Los sistemas capaces de afectar negativamente a la seguridad o a los derechos fundamentales se consideran de alto riesgo. Entre ellos se incluyen: a) los sistemas de IA sujetos a la normativa de seguridad de productos (automóviles, sistemas de aviación, dispositivos médicos, ascensores, etc.); y b) los sistemas de IA relacionados con la gestión del funcionamiento de infraestructuras críticas, la gestión de la inmigración, el acceso a servicios públicos esenciales, la gestión de prestaciones estatales, etc.

en lugares de trabajo y escuelas, la puntuación social y determinados sistemas de identificación biométrica a distancia[61].

En lo que se refiere al ámbito electoral, en primer lugar, en el nuevo Reglamento se prohíben los riesgos inaceptables, así como los que amenazan la seguridad o los derechos y libertades de los ciudadanos, incluidas las prerrogativas relacionadas con el ejercicio libre, consciente y autodeterminado de la participación política. En esta categoría se incluyen las aplicaciones capaces de manipular el comportamiento humano[62] e identificar o proporcionar información sobre las vulnerabilidades de determinados grupos, así como las circunstancias especiales que implican la categorización biométrica o la videovigilancia masiva por parte de las autoridades en espacios públicos.

También afectan a los procesos electorales los sistemas de alto riesgo, que amenazan infraestructuras críticas y pueden interferir en los derechos de las personas, como los relacionados con los derechos democráticos (gestión del censo electoral, reconocimiento de firmas en el voto por correo o sistemas de identificación biométrica para el acceso al voto). Todos los sistemas que utilicen estas técnicas deberán garantizar: a) la gobernanza de los datos, de forma que mantengan estándares de calidad y estén libres de sesgos y discriminaciones; b) la seguridad y la supervisión humana en todos los ciclos[63] ; c) el cumplimiento de sus deberes de transparencia sobre el funcionamiento del sistema; d) el registro en una base de datos a nivel comunitario; y e) la superación del test de conformidad, con vistas a la obtención de la correspondiente certificación.

Por último, los sistemas de riesgo medio o bajo, como los asistentes virtuales o *chatbots* que no afectan directamente a la privacidad, inicialmente no suponen riesgos significativos para los derechos y libertades, aunque eventualmente puedan ser utilizados en aplicaciones de recomendación de voto (por cierto, cada vez más habituales). En esta dimensión, la medida básica garantiza la transparencia, para que los usuarios puedan entender cómo funcionan y sus principales características y puedan evitar sesgos ideológicos o partidistas.

---

[61] En cuanto a los plazos de cumplimiento, se espera que las normas prohibitivas entren en vigor a finales de 2024, mientras que las normas que imponen obligaciones a las empresas que desarrollan "modelos fundacionales" (modelos que sirven de base para otros productos de IA, como GPT-4) tendrán que cumplir la ley en el plazo de un año. Las demás obligaciones derivadas de la nueva legislación deberán cumplirse en un plazo de dos años.

[62] Ejemplos de estas prácticas son las técnicas de marketing y la publicidad subliminal, que se introducen en la conciencia de las personas para alterar sustancialmente su comportamiento de forma potencialmente perjudicial para sus intereses.

[63] "el ciclo de vida de la Ia incluía técnicamente las siguientes fases: 1. diseño, datos y modelización (planificación, recopilación de datos y construcción del modelo); 2. desarrollo y validación (entrenamiento y pruebas); 3. despliegue; 4. supervisión y perfeccionamiento (solución de cualquier problema que se produzca)" (Lage, F. (2022) Manual de Inteligência Artificial no Direito Brasileiro. 2. ed. Salvador: Jus Podivm, p. 62).

Además, con motivo de las elecciones al Parlamento Europeo de 2024, se adoptaron una serie de medidas que, aunque no tratan específicamente de la IA, contienen referencias concretas a sus posibles aplicaciones en las campañas electorales. Las medidas se derivan del "Plan de Acción Europeo para la Democracia"[64], que busca "empoderar a los ciudadanos y aumentar la resiliencia democrática en toda la Unión promoviendo elecciones libres y justas, reforzando la libertad de los medios de comunicación y combatiendo la desinformación". Entre las medidas que incluye el plan, cabe destacar las siguientes:

a) El Código Reforzado de Buenas Prácticas contra la Desinformación, adoptado en 2022,[65] que sustituye y refuerza el Código anterior, de 2018,[66] y fue firmado por 34 entidades, incluidas plataformas en línea, agencias de publicidad, verificadores de hechos, instituciones académicas y organizaciones de la sociedad civil. Este Código de buenas prácticas sobre desinformación, de carácter voluntario, se ha integrado en febrero de 2025 en el marco de la Ley de Servicios Digitales (DSA). Con su integración, la adhesión plena al Código puede considerarse una medida adecuada de mitigación de riesgos para los signatarios designados como VLOP y VLOSE en virtud de la DSA. Como tal, el Código se convertirá en un parámetro significativo para determinar el cumplimiento de la DSA. El cumplimiento de los compromisos en virtud del Código también formará parte de la auditoría independiente anual a la que están sujetas estas plataformas en virtud de la DSA. Sus compromisos, que serían de aplicación al uso de la IA, incluyen: desmonetizar la difusión de la desinformación; garantizar la transparencia de la publicidad política; reducir el comportamiento no auténtico utilizado para difundir la desinformación; cooperar con los verificadores de hechos; y proporcionar a los investigadores acceso a los datos. Dentro del grupo de trabajo creado para supervisar su aplicación, destaca la creación de un Centro de Transparencia[67], que recoge informes de las plataformas que forman parte de él[68].

b) El Reglamento sobre transparencia y segmentación de la publicidad política[69] busca apoyar unas elecciones libres y justas y también afecta a actividades para las que se está utilizando ya IA. De esta manera: a) amplia el concepto de publicidad

[64] Disponible en: [https://commission.europa.eu/document/download/5d470456-641c-4248-951c-0ff1d52627fe_en?prefLang=es], consultado el: 17.09.2024.

[65] Disponible en: [https://digital-strategy.ec.europa.eu/news-redirect/749495], consultado el: 17.09.2024.

[66] Disponible en: [https://ec.europa.eu/newsroom/dae/redirection/document/87534], consultado el: 17.09.2024.

[67] Disponible en: [https://disinfocode.eu], consultado el: 11.04.2024.

[68] Disponible en: [https://disinfocode.eu/reports-archive/?years=2024], consultado el: 11.04.2024.

[69] Disponible en: [https://data.consilium.europa.eu/doc/document/PE-90-2023-INIT/es/pdf], consultado el: 11.04.2024. Para un estudio detallado del texto García Mahamut, R. (2023) Elecciones, protección de datos y transparencia en la publicidad política: la apuesta normativa de la UE y sus efectos en el ordenamiento español. Revista Española de la Transparencia, Núm. 17. Número Extraordinario, p. 75-105.

política; b) reduce la fragmentación jurídica y elimina los obstáculos habituales de los servicios transfronterizos; c) aumenta las obligaciones de transparencia de la publicidad política (definiendo como tal la que realizan los partidos políticos pero también los anuncios temáticos), que deberá identificarse como tal y ofrecer información básica sobre el patrocinador, las elecciones a las que está vinculada, el importe invertido y las técnicas de segmentación utilizadas y d) restringe el uso de técnicas de microsegmentación y amplificación para este tipo de publicidad política, que a partir de ahora sólo podrá realizarse con datos recabados directamente del sujeto, con su consentimiento explícito y distinto para este uso. También, e) prohíbe, en cualquier caso, la microsegmentación basada en datos personales que afecten a la raza, la etnia o las opiniones políticas. Y, por último, en un esfuerzo por evitar injerencias externas, f) prohíbe la contratación de publicidad por parte de organizaciones de terceros países durante los tres meses anteriores a la votación.

c) La DSA también tiene un efecto directo en las elecciones, ya que regula la moderación de los contenidos en línea y armoniza las normativas nacionales sobre contenidos ilegales, publicidad y desinformación, algo habitual, como hemos visto, en campaña electoral. En particular: a) establece mecanismos que permiten a los usuarios denunciar este tipo de contenidos[70]; b) garantiza que las decisiones tomadas por los moderadores de las plataformas puedan ser impugnadas y c) refuerza la transparencia de las plataformas, incluyendo, por ejemplo, la transparencia de los algoritmos utilizados para las recomendaciones. La parte que afecta más directamente al uso de IA en campaña corresponde a las plataformas muy grandes (VLP), aquellas que alcanzan a más del 10% de la población de la UE[71]. Estas asumen la obligación de analizar los riesgos sistémicos relacionados con los procesos electorales, entre los que la desinformación ocupa un lugar prominente[72], lo que ha dado lugar a una serie de recomendaciones específicas para las elecciones al Parlamento Europeo de 2024, entre ellas: a) reforzar sus procesos internos en función del riesgo potencial; b) mejorar su capacidad para dar respuesta a estos comportamientos; c) implementar medidas de mitigación de riesgos; d) promover la información oficial sobre procesos electorales, por ejemplo con iniciativas de alfabetización mediática y e) adaptar sus sistemas de recomendación para empoderar a los usuarios y reducir la monetización y viralidad de contenidos que amenacen la integridad de los procesos electorales. Además, según el nuevo Reglamento sobre transparencia y orientación de la publicidad política, comentado anteriormente, la publicidad política debe estar claramente etiquetada como tal, registrando explícitamente cuándo se produce el uso de IAG.

---

[70] Cada país debe certificar "trusted flaggers", o alertadores confiables, responsables de detectar contenidos potencialmente ilegales (entre ellos contenidos ilegales como *deepfakes* destinados a desinformar en campañas) y alertar a las plataformas en línea, que se obligan a tratar estas alertas de manera prioritaria. Son entidades certificadas por los coordinadores nacionales de servicios digitales (DSC).

[71] Disponible en: [https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses], consultado el: 11.04.2024.

[72] Arts. 34 y 35 DSA.

La Comisión ha tomado medidas concretas en el contexto de las elecciones y de la integridad de la información en aplicación de la DSA[73]. La evaluación inicial de la Comisión, así como los informes iniciales del grupo de trabajo del European Digital Media Observatory (EDMO) sobre las elecciones europeas de 2024[74] coinciden en señalar que, si bien circuló información errónea y desinformación en torno a las elecciones, no se produjeron incidentes de desinformación importantes o sistemáticos que perturbaran las elecciones. Aún así durante este periodo se han enviado más de cincuenta solicitudes de información (RFI) a los VLOPSE, una parte de ellas relacionadas con las medidas de mitigación del riesgo electoral y la IA generativa (como las llamadas «alucinaciones» en las que la IAG proporciona información falsa, la difusión viral de *deepfakes*, así como la manipulación automatizada de servicios que pueden inducir a error a los votantes)[75]. Entre estas se encuentra la solicitud de información a Microsoft sobre los riesgos que presenta su chatbot de IA, Copilot y a Google Search, expresando su preocupación sobre la "manipulación automatizada de servicios que puede engañar a los votantes". También ha solicitado información a Meta, X, Snapchat, Tik Tok y YouTube por no hacer lo suficiente para proteger a los usuarios de las campañas de desinformación[76]. Por último, la Comisión ha abierto procedimientos formales contra X[77] y Meta[78] por incumplimientos de la DSA durante el proceso electoral. En el ámbito nacional una buena parte de los coordinadores

[73] En abril de 2024, en vísperas de las elecciones europeas, la Comisión publicó unas directrices para los proveedores de VLOPSE, previa consulta pública, en las que se recomiendan medidas de mitigación de riesgos para la integridad electoral (Commission 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). La Comisión organizó una prueba de resistencia en forma de ejercicio de simulación para preparar a los VLOPSE, las organizaciones de la sociedad civil, los DSC y las instituciones europeas para escenarios de manipulación de la información, y ejercitar respuestas coordinadas en el marco de la DSA y las directrices electorales. (Commission stress tests platforms' election readiness under the Digital Services Act – European Commission) y una serie de diálogos con los actores involucrados (DSA Election Readiness - Roundtable with Platforms, Search Engines, and Digital Service Coordinators – European Commission), así como un grupo de trabajo ad hoc. (Report on the European Elections Digital Services Act And Code of Practice on Disinformation. European Board for Digital Services, 2024. Pags. 11-12). Disponible en: [https://ec.europa.eu/newsroom/dae/redirection/document/107587], consultado el: 17.09.2024.

[74] Disponible en: [https://edmo.eu/blog/eu-elections-2024-the-battle-against-disinformation-was-won-but-the-attrition-war-is-far-from-over/], consultado el: 17.09.2024.

[75] Disponible en: [https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-generative-ai-risks-6-very-large-online-platforms-and-2-very], consultado el: 17.09.2024.

[76] Report on the European Elections Digital Services Act And Code of Practice on Disinformation. European Board for Digital Services, 2024. Disponible en: [https://ec.europa.eu/newsroom/dae/redirection/document/107587], consultado el: 17.09.2024

[77] Disponible en: [https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709; Disponible en: [https://ec.europa.eu/commission/presscorner/detail/en/IP_24_3761], consultado el: 17.09.2024.

[78] Disponible en: [https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373], consultado el: 17.09.2024.

nacionales de servicios digitales (DSC) desarrollaron actuaciones específicas en esta materia[79].

d) Por último, la "Recomendación sobre Procesos Electorales Inclusivos y Resilientes en la UE" aborda la protección y la ciberseguridad de las infraestructuras relacionadas con las elecciones, que deben clasificarse como críticas, así como las bases de datos y los procesos, en línea con la propuesta de Ley de Resiliencia Cibernética. Junto a medidas para minimizar los riesgos de injerencia de terceros países como el control de la financiación de los partidos políticos y sus campañas, o el refuerzo de la transparencia de partidos y candidatos, incluye la adopción de códigos de conducta que faciliten la integridad electoral y campañas justas, promoviendo un discurso político inclusivo y prohibiendo comportamientos manipuladores, como la generación o difusión de falsedades (incluyendo *deepfakes*), o que inciten al odio, así como el rechazo al uso de tácticas, técnicas y procedimientos no auténticos para difundir o amplificar mensajes políticos, donde la IA juega un papel cada vez más importante; promoviendo mecanismos de control independientes para el cumplimiento de los compromisos adquiridos. En resumen, la UE ha creado un marco normativo que pretende evitar la desinformación y la injerencia extranjera y, dentro de su propuesta integral, trata de dar respuesta a la utilización de la IA en las campañas electorales.

Por otro lado, la Convención sobre IA y Derechos humanos, democracia y Estado de Derecho del Consejo de Europa[80], busca establecer un marco legal global que garantice que las actividades relacionadas con sistemas de inteligencia artificial (IA) respeten los derechos humanos, la democracia y el estado de derecho. Dirigido a la actuación de los Estados firmantes, incluye principios sobre dignidad humana, transparencia, responsabilidad, privacidad, y no discriminación. Tras definir los "sistemas de IA" como "sistemas basados en máquinas que, con objetivos explícitos o implícitos, infiere de los datos que recibe cómo generar salidas tales como predicciones, contenido, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales". En su artículo 5 establece la obligación de los firmantes de adoptar "medidas que garanticen que los sistemas de inteligencia artificial no se utilicen para socavar la integridad, independencia y eficacia de las instituciones y procesos democráticos, incluyendo el principio de la separación de poderes, respeto por la independencia judicial y acceso a la justicia", así como de "proteger sus procesos democráticos en el contexto de las actividades relacionadas con los sistemas de inteligencia artificial, incluyendo el acceso justo y la participación en el debate público, y la capacidad de las personas para formar libremente sus opiniones." Entre las respuestas, el artículo 16 establece un marco de gestión de riesgos e impactos para los sistemas de IA. Cada parte debe adoptar medidas para identificar, evaluar, prevenir y mitigar los riesgos que estos sistemas pueden suponer para los derechos humanos, la democracia y el

[79] Report on the European Elections Digital Services Act And Code of Practice on Disinformation. European Board for Digital Services, 2024. Pags. 13-15. Disponible en: [https://ec.europa.eu/newsroom/dae/redirection/document/107587], consultado el: 17.09.2024

[80] Disponible en: https://rm.coe.int/1680afae3c

estado de derecho. Estas medidas deben ser proporcionales al contexto, la gravedad y probabilidad de los impactos. Además, deben incluir monitoreo continuo y pruebas previas a su uso. También se prevé la posibilidad de imponer moratorias o prohibiciones a usos de la IA que sean incompatibles con estos valores.

El carácter incipiente de la regulación de la IA en el mundo, con excepciones puntuales como las señaladas, sólo ha alcanzado el ámbito electoral en Estados Unidos donde ya se han aprobado algunas normas dirigidas a limitar el uso de la IA en los procesos. En el ámbito federal la FCC, tras el uso de los audios falsos del Presidente Biden en *robocalls* durante las primarias de New Hampshire, ha declarado ilegales estos *robocalls* que utilizan voces generadas por IAG[81]. Además, algunos estados, tan ideológicamente diversos como California[82], Minnesota[83], Texas[84], Washington[85] y Florida[86], han aprobado nuevas leyes que prohíben o restringen de otro modo el uso de los *deepfakes* y otros medios engañosos en la publicidad electoral y los mensajes políticos.

Por un lado, estaría la priorización en la agenda judicial de los procedimientos relacionados con las elecciones y el establecimiento de procedimientos legales para los candidatos cuyas imágenes o voces sean utilizadas de manera engañosa, que incluyen medidas cautelares (California y Washington). Por otro la prohibición de determinados tipos de contenidos audiovisuales que alteren la realidad (*deepfakes*) en el periodo previo a la elección (90 días en Minnesota, 60 días en California y 30 días en Texas). En todos es necesaria la intención de dañar a un candidato o influir en el resultado de una elección, y se establecen diferentes penas según la gravedad del delito. Finalmente, en California, en Washington y en Florida se establece la obligación de etiquetar el contenido que haya utilizado IAG "en todo o en parte", exigiendo que además de la utilización de estas técnicas se genere la falsa apariencia de una persona real, y se pretenda atacar a un candidato o "engañar sobre una cuestión electoral". En el caso de California y Florida, se permite su distribución siempre que se incluya una advertencia indicando que el medio ha sido manipulado. Por último, se establece la responsabilidad de los patrocinadores de comunicaciones electorales que contienen medios sintéticos o no cumplen con el etiquetado obligatorio, pero no de los medios que los difunden, excepto en ciertas circunstancias y exime a los proveedores

[81] Disponible en: [https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf], consultado el: 4.4.2024

[82] Disponible en: [https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730], consultado el: 4.4.2024

[83] Disponible en: [https://www.revisor.mn.gov/bills/text.php?number=HF1370&type=bill&version=3&session=ls93&session_year=2023&session_number=0], consultado el: 4.4.2024

[84] Disponible en: [https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751F.htm], consultado el: 4.4.2024

[85] Disponible en: [https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/Session%20Laws/Senate/5152-S.SL.pdf?q=20231003125542], consultado el: 4.4.2024

[86] Disponible en: [https://www.flsenate.gov/Session/Bill/2024/919/BillText/er/PDF], consultado el: 4.4.2024

o usuarios de servicios de computación interactiva de ser tratados como el editor o portavoz de cualquier información proporcionada por otro proveedor de contenido de información, aunque permite que sean responsables en ciertas circunstancias.

5.4. La respuesta de los órganos electorales

Sin embargo, ante la ausencia de una regulación específica para las elecciones, y la insuficiencia de la autorregulación, algunos organismos electorales, como el caso del Tribunal Electoral (TE) de Panamá o el Tribunal Superior Electoral (TSE) Brasileño, han adoptado distintas medidas.

El TE de Panamá[87] en dos decretos del 23 de enero de 2024 que reglamenta la manipulación de medios digitales de forma masiva con el propósito de afectar el proceso electoral, como desarrollo del artículo 539 del Código Electoral, incluye entre las acciones que susceptibles de provocar esta manipulación, la creación de perfiles o contenidos falsos a través de IA[88].

En el caso de Brasil, ante la ausencia de un marco normativo —y en un escenario de riesgos inminentes, el TSE, aprovechando la prerrogativa inscrita en el artículo 57-J de la Ley de Elecciones (Ley nº 9.504/97[89]), aprobó, el 27 de febrero de 2024, un conjunto de reglas destinadas a disciplinar el uso de IA en las campañas, concretamente en los arts. 9º-B a 9º-H de la Resolución nº 23.610/2019, actualizada por la Resolución nº 23.372/2024. 9º-B a 9º-H de la Resolución nº 23.610/2019, actualizada por la Resolución nº 23.372/2024, dando así un paso importante en la defensa activa de la integridad de los procesos de renovación política y de la propia democracia brasileña. El texto normativo establece como puntos principales:

1. Usos prohibidos.

Hay usos que están estrictamente prohibidos, y pueden llegar a constituir abuso de poder económico o uso indebido de los medios de comunicación, lo que puede dar lugar a la anulación de candidaturas y mandatos, así como a la imposición de la pena de inelegibilidad durante ocho años. Esto incluye las *deepfakes*, independientemente de su finalidad —ya sean positivas o destinadas a atacar a candidatos contrarios— a

[87] Disponible en: [https://www.tribunal-electoral.gob.pa/sanciones-por-delitos-informaticos-electorales/]

[88] Decreto n.° 6 de 23 de enero de 2024 que modifica el artículo 228 del Decreto n.° 29 de 30 de mayo de 2022, que convoca a la Elección General del 5 de mayo de 2024 y aprueba su reglamentación y Decreto 7 de 23 de enero de 2024, que reglamenta la manipulación de medios digitales de forma masiva con el propósito de afectar la integridad del proceso electoral.

[89] "Artículo 57-J. El Tribunal Superior Electoral reglamentará lo dispuesto en los artículos 57-A a 57-I de esta Ley de acuerdo con el escenario y las herramientas tecnológicas existentes en cada momento electoral y promoverá, para los vehículos, partidos y demás entidades interesadas, la formulación y amplia divulgación de reglas de buenas prácticas relativas a las campañas electorales en Internet."

pesar de la dificultad para dictaminar su uso, así como la promoción y priorización pagada de información desinformativa contra la integridad del proceso electoral en los resultados obtenidos de las búsquedas de los usuarios, tanto en motores de búsqueda (Google, Bing u otros) como en otras plataformas de medios sociales (por ejemplo, búsquedas en plataformas de alojamiento de vídeos como YouTube, o redes sociales como Facebook, X o Instagram)[90].

2. Usos permitidos de la IA en la propaganda electoral.

La resolución establece dos tipos de usos permitidos de la IA en la propaganda electoral, guiados por reglas diferentes: El primer grupo incluye los usos ordinarios, por ejemplo, para realizar ajustes en imágenes y sonido o para crear viñetas y otros elementos gráficos. El uso de estas tecnologías es libre y no requiere identificación. La norma tiene sentido, ya que hoy en día cualquier fotografía tomada con un teléfono móvil, pasa automáticamente por un proceso de ajuste gráfico mediante herramientas de IA, algo que no suscita mayores reacciones en el público.

El segundo afecta a la creación de contenidos sintéticos o ajustes más avanzados, que requieren que la campaña informe claramente al electorado de que el material se ha producido utilizando IA. Encontramos así un nivel intermedio de regulación, que supone que la información transmitida a los receptores del mensaje les permitirá hacer un juicio más realista de lo que se presenta.

3. Restringir el uso de robots para mediar en el contacto con los votantes.

Se prohíben los *chatbots* y similares que pretendan hacerse pasar por los propios candidatos, dando la impresión al electorado de haber entablado una comunicación directa con esa persona.

4. Responsabilidad de las grandes tecnológicas.

Las grandes tecnológicas están obligadas a retirar inmediatamente los contenidos que contengan desinformación, discursos de odio, ideología nazi y fascista, así como contenidos antidemocráticos, racistas y homófobos estableciendo (9-H) que la efectiva remoción de contenido no exonera las responsabilidades de los usuarios involucrados, que posteriormente pueden ser multados en el ámbito de las elecciones. En este sentido, la supresión de contenidos no impediría el establecimiento acumulativo de

[90] "Apartado 1: Se prohíbe a los proveedores de aplicaciones que comercialicen cualquier forma de potenciación de contenidos, incluso en forma de priorización de resultados de búsqueda, que pongan este servicio a disposición de la difusión de hechos notoriamente falsos o gravemente descontextualizados que puedan afectar a la integridad del proceso electoral."

sanciones pecuniarias, siempre y cuando se observe la garantía de un proceso contradictorio y la plena defensa en un juicio posterior.

El artículo 9-D[91] impone a las plataformas la obligación de adoptar y publicar medidas para prevenir o reducir la circulación de narrativas desinformativas que puedan poner en peligro el buen desarrollo de las elecciones y establece una lista de medidas destinadas a señalar el cumplimiento del deber de diligencia.

El incumplimiento de la prohibición de la promoción y priorización pagada de información desinformativa contra la integridad del proceso electoral conlleva la obligación de reparar el ecosistema informativo mediante la promoción gratuita de mensajes que desmientan las noticias falsas o las aclaren (por ejemplo, añadiendo información maliciosamente omitida u otros elementos contextuales)[92], como notas aclaratorias, artículos de *fact-checking*, estudios especializados, documentos oficiales o informes públicos de cualquier tipo, a criterio de la autoridad judicial.

La orden faculta a las autoridades judiciales para que, mediante orden expresa, obliguen a los proveedores de aplicaciones de Internet a alimentar el repositorio creado, incorporando una cantidad considerable de información (artículo 9º-G, § 2º). 9º-G, § 2º).

6. **Conclusiones. Una respuesta global y estratégica**

En resumen, el desarrollo de la democracia digital —con la IA en su núcleo— cambia el comportamiento social, establece un nuevo entorno para la comunicación política y reconfigura las condiciones competitivas de la arena electoral. Implica un nuevo conjunto de retos sistémicos para las instituciones electorales y el conjunto de la sociedad y, en consecuencia, señala la necesidad de revisar los marcos jurídicos existentes, con la vista puesta en salvaguardar los supuestos de libertad, igualdad, integridad, transparencia y justicia. Comprender y desmitificar las amenazas, identificar y abordar las vulnerabilidades son pasos esenciales para mantener la soberanía a salvo de un nuevo marco de fraude, trampa y manipulación.

Para ofrecer una respuesta eficaz es necesario establecer un marco legal claro y sólido sobre el uso de la IA en campaña, sin delegarlo en las empresas del sector. Un marco que adopte una posición sobre: la protección de la privacidad; la responsabilidad del contenido producido con IA; los modelos de publicidad donde la IA desempeña un papel fundamental, para evitar que afecte a la libertad de decisión, aumentando la transparencia (con bibliotecas de anuncios políticos de acceso abierto)

[91] "Artículo 9-D. Es deber del proveedor de aplicaciones de Internet, que permita la difusión de contenidos político-electorales, adoptar y publicitar medidas para evitar o reducir la circulación de hechos notoriamente falsos o gravemente descontextualizados que puedan afectar la integridad del proceso electoral, entre ellas: [...]".

[92] "Apartado 3 La Corte Electoral podrá ordenar al proveedor de la aplicación la difusión, vía boosting y de forma gratuita, de contenidos informativos que diluciden un hecho notoriamente falso o gravemente descontextualizado previamente aumentado (*boosted*) de forma irregular, en la misma forma y con el mismo alcance que el contrato."

y posicionándose con claridad sobre el uso del microtargeting estableciendo limitaciones a su utilización o incluso planteando la prohibición al uso de estas técnicas en procesos electorales; el respeto a las garantías del debido proceso cuando se deje en manos de la IA las medidas de moderación y eliminación de contenido así como el uso de esta tecnología para luchar contra la desinformación (para garantizar que sea realmente independiente); el nivel de transparencia exigible (con medidas como las que evitan que los *bots* se presenten como personas identificando el contenido generado por máquinas); así como la rendición de cuentas, facilitando el acceso de investigadores, las iniciativas de verificación de datos y las organizaciones de la sociedad civil para evaluar el impacto de la IA en las campañas políticas en línea.

BIBLIOGRAFÍA

Libros

Alvim, F.F., Zilio, R.L., y Carvalho, V.O. (2023). *Guerras cognitivas na arena eleitoral: o controle judicial da desinformação*. Rio de Janeiro: Lumen Juris.

Alvim, F.F., Rubio, R. y Monteiro, V. A. (2024). Inteligência Artificial e eleiçôes de alto risco. Ciberpatologías e ameaças sistémicas da nova comunicaçao política. Rio de Janeiro: Lumen Juris.

Arias Maldonado, M. (2016). *Democracia Sentimental: política y emociones en el siglo XXI*. Madrid: Página Indómita.

Castells, M. (1998). The information age: economy, society and culture. Vol. III. End of millenium. Willey-Blackwell.

De Carreras, F. y Vallés, J.M. (1977), Las elecciones. Introducción a los sistemas electorales. Blume, Barcelona.

Kakutani, M. A morte da verdade: Notas sobre a mentira na era Trump. Rio de Janeiro: Intrínseca, 2018.

Kiffer, A., Giorgi, G. (2019) Ódios políticos e política do ódio. Lutas, gestos e escritas do presente. Bazar do Tempo, Rio de Janeiro.

Kissinger, H.A., Schmidt, E., y Huttenlocher, D. (2023). *La era de la Inteligencia Artificial y nuestro futuro humano*. Madrid: Anaya Multimedia.

Lassalle, J.M. (2021). *Liberalismo herido. Reivindicación de la libertad frente a la nostalgia del autoritarismo*. Barcelona: Arpa & Alfil.

López-Guerra, L. (1977). *Las campañas electorales en Occidente*. Barcelona: Ariel.

Moore, M. (2022). *Democracia hackeada: como a tecnologia desestabiliza os governos mundiais*. São Paulo: Editora Hábito.

Ramonet, I. (2022). *La era del conspiracionismo. Trump, el culto a la mentira y el asalto al Capitolio*. Buenos Aires: Siglo XXI.

Rubio Núñez, R., y Vela, R. (2017). *Parlamento Abierto: El parlamento en el siglo XXI*. UOC Editorial.

Sánchez Muñoz, Ó. (2020). *La regulación de las campañas electorales en la era digital. Desinformación y microsegmentación en las redes sociales con fines electorales*. Madrid: CEPC.
Sartori, G. (1989) Homovidens. La sociedad teledirigida. Taurus.
Snyder, T. (2017). *Sobre a tirania. Vinte lições do século XX para o presente*. São Paulo: Companhia das Letras.

Artículos en revistas

Norris, P. (2004). The evolution of campaign communications. Anais do congresso Political Communications in the 21st Century, University of Otago, New Zealand, Janeiro de 2004.
Rubio Núñez, R. (2018). "Los efectos de la posverdad en la democracia". *Revista de Derecho Político*, n. 103, UNED.
Tasioulas, J. (2019). "First step towards and Ethics of robots and Artificial Intelligence". *Journal of Practical Ethics*, 7(1), pp. 61-95.

Capítulos o artículos en libros

Arnaldo Alcubilla (2009). "El procedimiento electoral en leyes electorales autonómicas", en Gálvez Muñoz, L. (dir.), *El Derecho electoral de las Comunidades Autónomas. Revisión y Mejora*. Madrid: CEPC, p. 373.
Bowman, N.D., y Cohen, E. (2020). "Mental Shortcuts, Emotion and Social Rewards", en Zimdars, M., y Mcleod, K., *Fake news: understanding media and misinformation in the Digital Age*. Cambridge: The MIT Press, pp. 223-233.
Burguera Ameave, L., y Corbacho López, A. (2013). "El derecho al olvido de los políticos en las campañas electorales", en Corredoira, L., y Cotino Hueso, L. (eds.), *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*. Madrid: CEPC.
Burguera Ameave, L., y Rubio Núñez, R. (2015). "Información y propaganda. La comunicación política y electoral en la época del gobierno abierto", en Bel Mallén, J.I., y Corredoira Alfonso, L. (Dirs.), *Derecho de la información: el ejercicio del derecho a la información y su jurisprudencia*. Madrid: CEPC, pp. 291-318.
Caiani, M., y Susánsky, P. (2021). "Radical-right political activism on the web and the challenge for European democracy. A perspective from Eastern and Central Europe", en Giusti, S., y Piras, E. (eds.), *Democracy and Fake News. Information Manipulation and Post-Truth Politics*. New York: Routledge, pp. 173-187.
De Vega, P. (2017), "Democracia y Elecciones", en Obras escogidas, CEPC, Madrid, pp. 775-778. Publicado en ABC, 8 de marzo de 2000.
Metaxas, P. T. (2020) "Technology, propaganda and the limits of human intellect", en Zimdars, M., Mcleod, K. Fake news: understanding media and misinformation in the Digital Age. The MIT Press, Cambridge, pp. 245-256.

Salinas Olarte, M. (2023). "Teorías de la conspiración: un análisis socio-político", en Figueruelo Burrieza, A. (dir.), y Martín Guardado, S. (coord.), *Desinformación, odio y polarización*. Cizur Menor: Aranzadi, pp. 333-349.

Shoai, A., y López Molina, A. (2023). "Polarización e inteligencia artificial: una sistematización del conocimiento disponible", en Vázquez-Barrio, T., y Salazar García, I. (eds.), *Inteligencia artificial, periodismo y democracia*. Valencia: Tirant lo Blanch, pp. 247-264.

Recursos en línea

Benedicto XVI. (2011). "Mensaje del Santo Padre Benedicto XVI para la XLV Jornada Mundial de las Comunicaciones Sociales. Verdad, anuncio y autenticidad de vida en la era digital". Disponible en: https://www.vatican.va/content/benedict-xvi/es/messages/communications/documents/hf_ben-xvi_mes_20110124_45th-world-communications-day.html.

Bradshaw, S.; Howard, P. N. 82017). Troops, trolls and troublemakers: a global inventory of organized social media manipulation. Oxford Internet Institute: University of Oxford.https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf

Bradshaw, S. Howard, P. N. (2018). Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation. Oxford Internet Institute: University of Oxford. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2018/07/ct2018.pdf

Bradshaw, S. Howard, P. N. (2019). The Global Disinformation Order 2019. Global Inventory of Organised Social Media Manipulation. Oxford Internet Institute: University of Oxford. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf

Bradshaw, S. Bailey, H. Howard, P. N. (2020). Industrialized Disinformation 2020 Global Inventory of Organized Social Media Manipulation. Oxford Internet Institute: University of Oxford. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf

Consejo de Europa. (2022). "Artificial Intelligence and Electoral Integrity". Concept Paper. Disponible en: https://www.coe.int/en/web/electoral-management-bodies-conference/concept-paper-2022.

Foro Económico Mundial. (2024). *The Global Risks Report 2024: Insight Report, 19th Edition*. Disponible en: https://www.weforum.org/reports/global-risks-report-2024/.

Kofi Annan Foundation (2020). Protecting electoral integrity in the Digital Age. Koffi Annan Foundation, Geneve. Disponible en: https://www.kofiannanfoundation.org/wp-content/uploads/2024/04/Kofi-Annan-Commission-on-Elections-and-Democracy-in-the-Digital-Age-report-2020-english.pdf , consultado 23.6.2024

NIYAZOV, S. (2019). "The Real AI Threat to Democracy". Towards Data Science. Disponible en: https://towardsdatascience.com/democracys-unsettling-future-in-the-age-of-ai-c47b1096746e

Title

Does artificial intelligence redefine election campaigns and their democratic effects?

Summary

1. Electoral technology and its use in campaigning; 2. The technological threat; 3. The digitalization of electoral information (and disinformation); 4. Uses of AI in election campaigns; 5. First responses. 5.1 Self-regulation, 5.2 Legislative response, 5.3 Electoral bodies, 6. Conclusions,

Resumen

El uso de la inteligencia artificial (IA) en las campañas electorales está transformando significativamente el panorama político y democrático. La IA ha introducido nuevas dinámicas en los procesos electorales, impactando en la manera en que se realizan las campañas lo que puede suponer una amenaza para la integridad de los sistemas democráticos.

Las innovaciones tecnológicas afectan la manera en que se gestionan y ejecutan las campañas electorales. Desde los medios tradicionales como la radio, la televisión y el cine, hasta las plataformas digitales, la evolución tecnológica ha permitido una mayor personalización y efectividad en la comunicación política. La IA facilita el análisis de grandes volúmenes de datos, permitiendo campañas altamente segmentadas y personalizadas.

Al mismo tiempo, las amenazas tecnológicas son una preocupación creciente para la democracia. La manipulación de datos, la creación de perfiles falsos y los ataques cibernéticos son algunos de los riesgos que enfrentan los procesos electorales. Estas prácticas pueden afectar la transparencia y equidad de las elecciones, comprometiendo principios básicos como la libertad del voto. La digitalización amplifica tanto la información como la desinformación. La propaganda política se ha sofisticado, utilizando técnicas de IA para crear y difundir contenido desinformativo de manera más efectiva. Este fenómeno contribuye a la fragmentación y polarización de la opinión pública, y puede erosionar la confianza en el proceso democrático y las instituciones.

La IA se utiliza para mejorar la capacidad de persuasión o disuasión de los partidos políticos y candidatos. Permite la creación de estrategias de co-

municación más sofisticadas y la optimización de los recursos electorales. Sin embargo, también plantea desafíos éticos y prácticos, como la manipulación de la realidad a través de *deepfakes* y la segmentación extrema del electorado.

Las respuestas a los desafíos planteados por la IA en el ámbito electoral han sido diversas. Algunas plataformas tecnológicas han adoptado medidas de autorregulación, como la etiquetación de contenido generado por IA. Sin embargo, la autorregulación ha sido insuficiente, y se requiere una respuesta legislativa más sólida para proteger la integridad de los procesos electorales. En algunos países, ya se han implementado leyes que prohíben el uso de *deepfakes* en campañas electorales.

La IA ofrece tanto oportunidades como riesgos, y su impacto en la democracia depende de cómo se gestionen sus aplicaciones y se mitiguen sus efectos negativos. Es crucial establecer un marco regulatorio nacional e internacional claro que abarque el uso de la IA en campañas electorales. Este marco debe garantizar la transparencia, equidad y protección de los derechos electorales. La colaboración entre gobiernos, instituciones electorales, empresas tecnológicas y la sociedad civil es esencial para preservar la integridad y legitimidad de los procesos democráticos en la era digital.

Abstract

The use of artificial intelligence (AI) in election campaigns is significantly transforming the political and democratic landscape. AI has introduced new dynamics into electoral processes, impacting the way campaigns are conducted, which can pose a threat to the integrity of democratic systems. Technological innovations affect the way election campaigns are managed and executed. From traditional media such as radio, television and film, to digital platforms, technological evolution has enabled greater personalization and effectiveness in political communication. AI facilitates the analysis of large volumes of data, enabling highly segmented and personalized campaigns.

At the same time, technological threats are a growing concern for democracy. Data manipulation, false profiling and cyber-attacks are some of the risks faced by electoral processes. These practices can affect the transparency and fairness of elections, compromising basic principles such as the freedom to vote. Digitalization amplifies both information and disinformation. Political propaganda has become more sophisticated, using AI techniques to create and disseminate disinformative content more effectively. This phenomenon contributes to the fragmentation and polarization of public opinion and can erode trust in the democratic process and institutions.

AI is used to improve the persuasiveness and determent of political parties and candidates. It allows the creation of more sophisticated communication strategies and the optimization of electoral resources. However, it also poses ethical and practical challenges, such as manipulation of reality through deepfakes and extreme segmentation of the electorate.

Responses to the challenges posed by AI in the electoral field have been diverse. Some technology platforms have adopted self-regulatory measures, such as tagging AI-generated content. However, self-regulation has proved to be insufficient, and a more robust legislative response is required to protect the integrity of electoral processes. In some countries, laws prohibiting the use of deepfakes in election campaigns have already been implemented.
AI offers both opportunities and risks, and its impact on democracy depends on how its applications are managed and its negative effects mitigated. It is crucial to establish clear national and international regulatory framework covering the use of AI in electoral campaigns. This framework must ensure transparency, fairness and protection of electoral rights. Collaboration between governments, electoral institutions, technology companies and civil society is essential to preserve the integrity and legitimacy of democratic processes in the digital era.

Palabras clave

Inteligencia artificial; Tecnología; elecciones; campañas electorales; desinformación.

Keywords

Artificial Intelligence; Technology; elections; election campaigning; disinformation.