IVADO

Initiative IA + Société
AI + Society

La IA en las urnas

Cuatro medidas para salvaguardar la integridad electoral y defender la democracia[1]

Catherine Régis, Florian Martin-Bariteau, Jake Okechukwu Effoduh, Juan David Gutiérrez, Gina Neff, Carlos Affonso Souza y Célia Zolynski

Por qué la IA y las elecciones son un tema crucial

Las tecnologías llevan mucho tiempo influyendo en las elecciones, tanto positiva como negativamente, determinando sus resultados y la calidad del debate público que las rodea. Por ejemplo, Internet permite a los ciudadanos organizarse con más eficacia que nunca, dándoles poder para defender ideas y causas concretas, pero también es un formidable canal de desinformación.

El auge de la inteligencia artificial (IA) presenta nuevas e importantes amenazas, como la multiplicación de ultra falsificaciones (deepfakes), el aumento de los riesgos de ciberseguridad, la aparición de agentes persuasivos manipuladores y la proliferación de datos sintéticos y cuentas falsas. Al mismo tiempo, la IA ofrece a los actores políticos una poderosa herramienta para conectar con los votantes, influir en la opinión pública y moldear el flujo de información. Al aprovechar las tendencias existentes en las elecciones, la IA tiene el potencial de remodelar profundamente el proceso democrático e influir en los resultados electorales. Sin embargo, sin medidas proactivas, la IA podría exacerbar tendencias preocupantes como la polarización política y la disminución de la confianza en la democracia.

Los gobiernos deberían tomar medidas decisivas en relación con la IA, especialmente en un momento en que las democracias de todo el mundo se enfrentan a crecientes desafíos y ataques a sus elecciones. Actuando en varios frentes, apuntalarán los sistemas democráticos, mejorarán la confianza en la sociedad y garantizarán que la IA sea aprovechada de forma responsable para mejorar la integridad de las elecciones.

Puntos Clave

- → Ejemplos recientes de Brasil, Rumanía, Gabón, Estados Unidos y otros países muestran cómo el uso de la IA por parte de actores políticos puede afectar negativamente la integridad electoral y la democracia.
- → Las naciones no suelen estar preparadas para los retos relacionados con la IA: muchas carecen de normas que regulen el uso de la IA en las elecciones, los partidos políticos no se han puesto de acuerdo sobre prácticas electorales justas en la era de la IA y la mayoría de las jurisdicciones no pueden contrarrestar eficazmente los ataques realizados con IA en contra de sus instituciones democráticas.
- → Recomendamos cuatro acciones: los Estados deberían actualizar las normas electorales (por ejemplo, para prohibir los contenidos engañosos generados con IA); los partidos políticos deberían adoptar un código de conducta con directrices claras sobre el uso responsable de la IA en actividades políticas; las autoridades electorales deberían establecer equipos independientes para prevenir y responder a las perturbaciones provocadas con IA; y, a nivel internacional, los gobiernos deberían establecer Guardianes Electorales Internacionales de IA y protocolos para abordar las interferencias transfronterizas.

Cómo la IA amenaza las elecciones y la democracia

Hay muchas formas en las que el uso de la IA por parte de los actores políticos -tanto locales como extranjeros- puede acabar afectando negativamente la integridad de las elecciones y la democracia.

Por ejemplo, en octubre de 2024 se celebraron elecciones en Brasil y un estudio del Digital Forensic Research Lab descubrió que, en los seis meses anteriores al día de las elecciones, los políticos locales o sus partidarios utilizaron IA al menos 75 veces para producir imágenes sintéticas, contenido de audio o vídeos para impulsar sus candidaturas o socavar a sus oponentes. En concreto, cinco candidatas fueron víctimas de pornografía ultra falsificada[2], un fenómeno cuyo impacto suele ser disuadir a las mujeres de asumir cargos públicos[3].

El Servicio de Inteligencia Exterior de Rumanía informó en diciembre de 2024 que Rusia había apuntado a ese país en un intento de influir en sus elecciones presidenciales. En primer lugar, Rusia utilizó propaganda prorrusa de extrema derecha y contenidos generados por IA que difundió a través de una amplia red de canales de redes sociales y cuentas generadas por IA. En segundo lugar, con la ayuda de la IA (que puede ayudar a desarrollar programas maliciosos que eluden las defensas de ciberseguridad), Rusia presuntamente organizó unos 85.000 ataques contra la Autoridad Electoral Permanente de Rumanía para acceder a sus bases de datos. La injerencia rusa llevó finalmente al Tribunal Constitucional de Rumanía a anular la primera vuelta de las elecciones presidenciales[4].

En la campaña electoral de 2023 en Gabón, estalló una polémica mientras los votantes se preparaban para una histórica votación triple: presidencial, legislativa y local. Casi al final de la campaña, aparecieron en Internet grabaciones de audio en las que supuestamente dos destacadas figuras de la oposición hablaban de estrategias, alianzas y apoyo externo. El presidente en funciones acusó a la oposición de "fomentar un levantamiento popular", mientras que la coalición opositora condenó las grabaciones como un "uso infame de la IA". El caso de Gabón pone de relieve cómo el auge de la IA complica el debate público, haciendo cada vez más difícil para los votantes distinguir la realidad de la ficción[5].

Por último, los expertos probaron los principales modelos de IA durante la campaña de las elecciones presidenciales de Estados Unidos de 2024 para comprobar su rendimiento a la hora de ofrecer información precisa sobre las elecciones. Estas pruebas mostraron discrepancias con respecto a la información en diferentes idiomas, y frente a los compromisos asmidos por las empresas de IA con la información electoral precisa y el rendimiento de sus modelos[6].

Estos ejemplos muestran cómo las naciones y los gobiernos a menudo no están preparados para afrontar los retos que plantea el auge de la IA. Nuestras recomendaciones sugieren formas de evitar o mitigar las repercusiones negativas que las tecnologías emergentes tienen en las elecciones.

Las elecciones locales son especialmente vulnerables a la influencia de la IA, ya que las democracias locales carecen a menudo de los recursos y salvaguardias necesarios para contrarrestar sus riesgos con eficacia.

Primer reto
Muchos Estados aún no han adoptado normas que regulen el uso de la IA en las elecciones

La ausencia de normas claras y específicas que regulen el uso de la IA en las elecciones crea inseguridad jurídica, lo que dificulta a las autoridades la atribución de responsabilidades o la adopción de medidas eficaces contra los abusos.

Muchas normas electorales de todo el mundo se adoptaron años antes de que la IA generativa se hiciera pública y se utilizara ampliamente. Como resultado, a menudo son demasiado amplias para abordar los riesgos únicos que plantea la IA. Por ejemplo, la mayoría de las legislaciones carecen de definiciones de "medios sintéticos" o "contenido generado por IA" y no definen los límites de su uso en el contexto de las elecciones.

Pocos órganos legislativos han adoptado o incluso debatido propuestas sobre normas electorales que aborden específicamente los retos de la IA en las elecciones. En el Reino Unido, por ejemplo, las leyes vigentes sobre difamación se centran en proteger a las personas de declaraciones falsas, pero son ambiguas cuando se trata de imágenes o vídeos falsos[7].

Unas normas claras y armonizadas son esenciales para garantizar la rendición de cuentas, mejorar la

transparencia y permitir intervenciones oportunas. Al colmar estas lagunas normativas, los tomadores de decisiones públicas (policymakers) pueden proporcionar salvaguardias sólidas para mantener la integridad de los procesos democráticos y reducir la creciente inseguridad asociada a los retos electorales impulsados por la IA.

Acción 1
Los Estados deberían actualizar las normas electorales

Los Estados deberían actualizar las normas electorales para garantizar que los políticos, los partidos políticos y las empresas tecnológicas, así como los votantes, sepan con precisión:

- **cómo pueden utilizarse los medios sintéticos para las actividades relacionadas con las elecciones;**
- **qué usos de los sistemas de IA están prohibidos o limitados en el contexto de las elecciones; y**
- **cómo se asigna la responsabilidad cuando se incumplen los deberes establecidos por las normas electorales.**

Para garantizar que la libertad de comunicación política no se vea restringida de forma significativa, las nuevas normas electorales deberían ser proporcionales al riesgo que pretenden evitar. Las autoridades independientes que supervisen el uso de IA en las elecciones necesitarán conocimientos técnicos y financiación adecuados para aplicar eficazmente estas normas.

Las jurisdicciones deberían aclarar las definiciones de términos clave, como datos sintéticos, IA generativa, contenido de IA generativa e información engañosa o que induce a error, y evaluar la necesidad de modificar aspectos puntuales de sus normas actuales. Además, deberían considerar seriamente la adopción de las siguientes normas obligatorias:

- **Debería prohibirse el uso, la publicación, la difusión o la circulación de contenidos engañosos generados por IA para influir en las elecciones. Por ejemplo, los Estados deberían considerar la posibilidad de prohibir el uso de imágenes, vídeos o audio generados por IA que retraten a candidatos o campañas de referéndum de forma falsa o engañosa, o que amplifiquen información errónea sobre un candidato, una campaña de referéndum o el proceso electoral;**
- **Los políticos y los partidos políticos deberían tener que cumplir obligaciones de transparencia, como etiquetar las imágenes, clips de audio y vídeos generados por IA que se utilicen, publiquen, proyecten o difundan en las elecciones. Para crear o mejorar estas etiquetas, los Estados deberían considerar la investigación científica y recabar la opinión del público. Las etiquetas deberían ser fáciles de reconocer por los ciudadanos, teniendo en cuenta aspectos como el diseño visual, la redacción, el tamaño, la duración, la posición y el momento en el que aparecen;**
- **Los Estados deberían obligar a las plataformas en línea a aplicar políticas de etiquetado para los anuncios políticos generados por IA, y a crear y aplicar estrictamente normas de moderación de contenidos para frenar la difusión de contenidos nocivos generados por IA.**

Las normas electorales deberían cubrir los chatbots, que pueden producir información engañosa sobre elementos clave de unas elecciones, como la ubicación de los colegios electorales, qué documentos se necesitan para votar o los antecedentes penales de los candidatos[8].

Segundo reto
Los partidos políticos no se han puesto de acuerdo sobre lo que constituyen unas elecciones libres y justas en la era de la IA

Los partidos políticos y los candidatos pueden ahora aprovechar las herramientas de IA para crear sofisticadas ultra falsificaciones (deepfakes), generar contenidos engañosos a gran escala, micro-focalizar a los votantes con desinformación personalizada o manipular el discurso público a través de cuentas automatizadas.

En ausencia de regulación, directrices claras o marcos éticos, existe el riesgo de que los partidos políticos utilicen la IA de forma que contribuya a socavar la confianza de los votantes, difundir información falsa e influir injustamente en los resultados electorales.

Sin unas normas consensuadas, los partidos políticos podrían sentirse obligados a intensificar el uso de herramientas de IA de forma cada vez más agresiva para evitar quedar por detrás de sus oponentes. La presión política podría crear una espiral en la que los partidos priorizaran el uso de la IA para ganar a cualquier precio sobre el mantenimiento de la integridad electoral.

Acción 2
Los partidos deberían adoptar un código de conducta como punto de partida para asumir la responsabilidad del comportamiento político en la era de la IA

Los códigos de conducta pretenden que los actores políticos acepten comprometerse con unas elecciones libres y justas adoptando determinados comportamientos o evitando otros. Los códigos de conducta sobre IA suelen apoyar la transparencia y la honestidad en el uso de esta tecnología con fines electorales.

En algunas jurisdicciones ya existen códigos de este tipo. Por ejemplo, en 2023, cinco partidos suizos se comprometieron a ser transparentes en el uso de la IA y a no utilizarla con fines despectivos. Para las elecciones al Parlamento Europeo de 2024, los partidos europeos aprobaron conjuntamente un código de conducta con disposiciones específicas que regulan el uso de la IA. En países como el Reino Unido y en entidades subnacionales se han realizado esfuerzos para desarrollar códigos de este tipo.

Los códigos de conducta sobre el uso de la IA con fines electorales deberían comprometer a los partidos a:

- **no utilizar herramientas de IA para producir contenidos materialmente engañosos o inducir a error a los votantes;**
- **etiquetar claramente los contenidos cuando las partes recurran a la IA de forma no trivial (los vacíos regulatorios señalados anteriormente y la urgencia de esta cuestión);**
- **no amplificar contenidos sintéticos materialmente engañosos, y denunciar los malos comportamientos tanto en la publicación como en la amplificación de contenidos engañosos;**
- **dar directrices claras y formación adecuada al personal del partido, los miembros de las campañas, los activistas y los simpatizantes del partido sobre el uso de las herramientas de IA para hacer campaña;**
- **abstenerse de producir, utilizar o difundir contenidos engañosos, incluidas cuentas falsas, bots automáticos o chatbots, para manipular la opinión de los votantes;**
- **introducir "capas de moderación" en sus chatbots para dirigir a los usuarios de Internet hacia información electoral oficial; y**
- **comprometerse a supervisar, auditar y revisar tras las elecciones el uso que hacen de la IA y de las herramientas basadas en ella.**

Tercer reto
La mayoría de las jurisdicciones no están preparadas para los ataques realizados con IA contra sus elecciones e instituciones democráticas

Los gobiernos han desarrollado estrategias y mecanismos para hacer frente a crisis graves como catástrofes naturales, disturbios civiles o pandemias. Sin embargo, la mayoría de los gobiernos no están preparados para enfrentarse a ataques realizados con IA en contra la integridad de sus elecciones e instituciones democráticas.

Enfrentarse con éxito a las amenazas a la integridad electoral impulsadas con el uso de IA es un reto polifacético.

En primer lugar, muchos gobiernos carecen de sistemas de supervisión exhaustivos para detectar la desinformación generada por IA, las ultra falsificaciones (deepfakes) y otras campañas de influencia automatizadas dirigidas a sus procesos democráticos. Esta brecha de conocimiento se ve agravada por la insuficiencia de mecanismos de colaboración entre las partes interesadas, como organismos gubernamentales, plataformas de redes sociales, organizaciones de noticias y grupos de la sociedad civil. Cuando se detectan actividades sospechosas, a menudo no existe un protocolo claro para compartir información o coordinar una respuesta.

En segundo lugar, muchos funcionarios electorales carecen de los conocimientos de IA necesarios para distinguir las amenazas, lo que les deja mal equipados para actuar. Este déficit de capacidad suele extenderse a todo el ecosistema democrático. Por ejemplo, los trabajadores electorales y los observadores electorales, que actúan como defensores de primera línea de la integridad electoral, suelen recibir una formación mínima sobre las amenazas digitales y pueden tener dificultades para responder a las preguntas de los votantes sobre el contenido generado por IA o los intentos de manipulación.

En tercer lugar, los organismos públicos carecen a menudo de la infraestructura técnica, los conocimientos humanos y la capacidad necesarios para vigilar y contrarrestar eficazmente los ataques impulsados con el uso de IA. Sin ellos, las jurisdicciones se ven obligadas a reaccionar ante los incidentes en función de las necesidades, en lugar de aplicar estrategias de defensa proactivas.

Acción 3
Las autoridades electorales deberían crear un equipo interdisciplinar independiente encargado de prevenir y responder a las perturbaciones electorales causadas por la IA

Las autoridades electorales deberían contar con un equipo multifuncional independiente que opere bajo supervisión judicial. Este equipo debería contar con el apoyo de todas las partes interesadas en los procesos democráticos y electorales de una jurisdicción. Debería tener vínculos adecuados con los actores del entorno mediático, las plataformas en línea y otras entidades regionales o internacionales pertinentes. También debería incluir a representantes de los partidos políticos para garantizar que los protocolos de emergencia y mitigación se consideren justos y equilibrados.

El equipo debería operar dentro y fuera del ciclo electoral para mantener la vigilancia sobre los ataques a la democracia. Sería responsable de desarrollar un plan de respuesta público y exhaustivo para las amenazas asociadas a la IA en contra de las elecciones. El Plan de Respuesta Electoral a la IA definiría marcos claros de evaluación, responsabilidades, enfoques de comunicación, etc. Este enfoque se basa en estrategias de preparación ante emergencias establecidas en campos como la gestión de crisis de salud pública, la respuesta ante desastres naturales y la preparación ante incidentes de ciberseguridad, que han implementado con éxito sistemas de alerta temprana, protocolos de información, divulgación obligatoria de incidentes, acuerdos para compartir recursos y equipos de respuesta rápida.

Todos los actores del ecosistema mediático y de Internet deberían participar en la implementación del plan de respuesta para limitar la propagación de un atentado y alertar a los ciudadanos.

Las autoridades electorales deberían llevar a cabo ejercicios de mesa o simulacros para permitir a los actores comprender cómo puede desplegarse y

utilizarse la IA, identificar y probar el plan de respuesta y las reacciones concretas a los incidentes, e identificar las posibles vulnerabilidades que podrían explotar los actores deshonestos.

El Plan de Respuesta Electoral debe tener en cuenta los derechos fundamentales de los ciudadanos para protegerse de las amenazas de vigilancia o control de la expresión política.

Para garantizar que las perturbaciones electorales causadas por la IA sean contrarrestadas eficazmente, debe impartirse una formación adecuada sobre IA y ciberseguridad a todos los actores del ecosistema democrático y electoral, incluidos los voluntarios de los puestos de votación y observadores de los colegios electorales.

Cuarto reto
La interferencia electoral apoyada por la IA a menudo implica a actores encubiertos que operan en múltiples jurisdicciones

La naturaleza transnacional de muchos ataques electorales impulsados por el uso de IA explica por qué es difícil para las jurisdicciones individuales hacerles frente por sí solas de manera eficaz. Este problema se complica por la asimetría de recursos y conocimientos entre los gobiernos, ya que algunos no tienen la experiencia, las herramientas, los recursos o la capacidad necesarios para detectar y contrarrestar adecuadamente las amenazas electorales impulsadas por el uso de IA.

Sin protocolos internacionales armonizados, es difícil exigir responsabilidades a los autores debido a las diferencias en los sistemas jurídicos, las capacidades de investigación y las fronteras jurisdiccionales.

Los Estados democráticos deberían reconocer que el ataque a una democracia es un ataque a los principios que unen a todas las democracias. Por lo tanto, la acción colectiva es esencial para proteger los valores democráticos compartidos, aumentar la confianza de los ciudadanos y garantizar la integridad de las elecciones en todo el mundo.

Acción 4
Los Estados deberían establecer Guardianes Electorales Internacionales de IA y protocolos internacionales de asistencia jurídica mutua en caso de injerencia electoral relacionada con la IA

Los Estados deberían crear una plataforma y una unidad internacional centralizada para conocer y reaccionar a los casos de injerencia electoral relacionada con la IA: los Guardianes Electorales Internacionales de IA.

Estarían formados por expertos multidisciplinares e instituciones comprometidas con la detección, la lucha y la mitigación de las interferencias electorales provocadas por la IA. Servirían como recurso técnico para los países vulnerables a la interferencia electoral mediante IA. Ofrecerían experiencia, herramientas y colaboración para hacer frente a las amenazas electorales transnacionales. Los Guardianes Electorales Internacionales de IA también ofrecerían apoyo en situaciones de crisis mediante el despliegue de equipos de respuesta rápida para prestar asistencia durante acontecimientos electorales activos y proporcionarían estrategias de supervisión y mitigación en tiempo real en escenarios de alto riesgo.

La creación de los Guardianes Electorales Internacionales de IA podría surgir de las iniciativas existentes destinadas a prestar asistencia electoral o a proteger a los países contra los posibles perjuicios de la IA, o estar en consonancia con ellas. Por ejemplo, podrían adoptarse medidas para proporcionar recursos nuevos o mejorados en materia de IA (por ejemplo, expertos ad hoc o especialistas

permanentes) asignar competencias (por ejemplo, técnicas o jurídicas) a la División de Asistencia Electoral de la ONU[9], que ayuda a los Estados miembros a celebrar elecciones que expresen legítimamente la voluntad del pueblo y sean consideradas creíbles por las partes interesadas nacionales. La incipiente Red Internacional de Institutos de Seguridad de la IA podría aprovecharse para esta iniciativa con el fin de formar a los Guardianes Electorales Internacionales de IA y desplegarlos por todo el mundo en misiones específicas.

Cuando se requiera la experiencia de la industria, los Guardianes Electorales Internacionales de IA podrían contar con el apoyo de actores del sector privado, como las empresas de IA y plataformas que respaldan el Acuerdo Tecnológico para Combatir la Interferencia Electoral Generada por IA.[10]

Recurrir a mecanismos de asistencia jurídica mutua también será esencial para investigar y enjuiciar los casos de interferencia electoral impulsada por la IA, ya que esto facilitará la cooperación sin fisuras de los actores a través de las jurisdicciones, ayudará a recopilar y compartir pruebas admisibles procedentes de múltiples países, y garantizará que los autores que utilizan la IA para manipular las elecciones a nivel transnacional no puedan explotar las fronteras jurisdiccionales para eludir la rendición de cuentas.

Estos mecanismos judiciales ya han abordado eficazmente otros retos transnacionales que requieren cooperación transfronteriza e intercambio de pruebas, como la lucha contra la ciberdelincuencia, el fraude digital, el terrorismo, la delincuencia organizada, las violaciones de los derechos humanos y los crímenes de guerra.

Estos mecanismos internacionales deberán ser transparentes para garantizar la salvaguardia de los derechos fundamentales.

Conclusión

El impacto de la IA en la democracia no está grabado en piedra.

Aunque este informe se ha centrado en los riesgos, la IA podría reforzar las democracias. Los funcionarios electorales podrían utilizar herramientas de IA para gestionar tareas complejas de forma eficiente. Estas herramientas podrían hacer el voto más accesible e impulsar la participación cívica. Por ejemplo, durante las controvertidas elecciones de 2024 en Pakistán, la IA permitió al partido de un líder de la oposición encarcelado enviar mensajes de audio a los votantes y movilizarlos a pesar de las restricciones.[11] De cara al futuro, los defensores de la democracia deberían estudiar cómo la IA puede mejorar los sistemas democráticos.

Ahora, sin embargo, la prioridad es proteger a las democracias de una amenaza acuciante: los agentes deshonestos, tanto nacionales como extranjeros, que hacen un uso indebido de la IA.

Para ello es necesario actuar a dos niveles.

Dentro de los países, los Estados deberían actualizar sus leyes, los partidos políticos deberían trabajar juntos y las autoridades electorales deberían prepararse para defender la integridad democrática frente a quienes abusen de la IA.

La cooperación entre países es esencial. Ninguna nación puede enfrentarse sola a los retos de la IA. Los países deberían armonizar sus leyes sobre la interferencia electoral posibilitada por la IA. Esto reforzará las defensas individuales y creará una resistencia colectiva contra los intentos de socavar la democracia en todo el mundo.

Si tomamos estas medidas hoy, crearemos sistemas democráticos más fuertes, inclusivos y fiables para el mañana.

Notas

1. La versión original de este texto fue producida en inglés bajo el título *AI in the Ballot Box*. La traducción al español fue realizada por el profesor Juan David Gutiérrez, de la Universidad de los Andes en Bogotá.
2. Farrugia, B. (2024, 26 de noviembre). Brazil's electoral deepfake law tested as AI-generated content targeted local elections. *DFRLab.* https://dfrlab.org/2024/11/26/brazil-election-ai-deepfakes
3. Para más información sobre cómo la IA plantea graves problemas para la seguridad de las mujeres, véase: United Nations Educational, Scientific and Cultural Organization. (2023). Technology-facilitated gender-based violence in an era of generative AI (World Trends in Freedom of Expression and Media Development Series). https://unesdoc.unesco.org/ark:/48223/pf0000387483
4. Harward, C. (2024, 6 de diciembre). Likely Kremlin-backed election interference against Romania threatens Bucharest's continued support for Ukraine and NATO. *Institute for the Study of War.* https://understandingwar.org/backgrounder/likely-kremlin-backed-election-interference-against-romania-threatens-bucharests
5. RFI. (2023, 23 de agosto). Élections au Gabon: polémique après des enregistrements supposés de candidats de l'opposition. *RFI.* https://www.rfi.fr/fr/afrique/20230823-%C3%A9lections-au-gabon-pol%C3%A9mique-apr%C3%A8s-des-enregistrements-suppos%C3%A9s-de-candidats-de-l-opposition
6. Palta, R., Angwin, J., & Nelson, A. (2024, 27 de febrero). How we tested leading AI models performance on election queries. *Proof.* https://www.proofnews.org/how-we-tested-leading-ai-models-performance-on-election-queries; ; Impelli, M. (2024, 31 de octubre). Voting rights groups warn about AI generating unfounded claims in Spanish. Newsweek. https://www.newsweek.com/2024-election-spanish-latino-voters-artifical-intelligence-concerns-1978170; Ott, H., & Lyons, E. (2024, 25 de junio). ChatGPT gave incorrect answers to questions about how to vote in battleground states. CBS News. https://www.cbsnews.com/news/chatgpt-chatbot-ai-incorrect-answers-questions-how-to-vote-battleground-states
7. Stockwell, S., Hughes, M., Swatton, P., & Bishop, K. (2024). AI-enabled influence operations: the threat to the UK general election. CETaS Briefing Papers. https://cetas.turing.ac.uk/sites/default/files/2024-05/cetas_briefing_paper_-_ai-enabled_influence_operations_-_the_threat_to_the_uk_general_election.pdf
8. Kaye, R. (2023, 5 de abril). Australian mayor readies world's first defamation lawsuit over ChatGPT content. Reuters. https://www.reuters.com/technology/australian-mayor-readies-worlds-first-defamation-lawsuit-over-chatgpt-content-2023-04-05
9. United Nations Department of Political and Peacebuilding Affairs. (2023). 2023 factsheet: electoral assistance. https://dppa.un.org/sites/default/files/electoral_assistance.pdf
10. AI Elections Accord (2024, 16 de febrero). A tech accord to combat deceptive use of AI in 2024 elections. https://www.aielectionsaccord.com/uploads/2024/02/A-Tech-Accord-to-Combat-Deceptive-Use-of-AI-in-2024-Elections.FINAL_.pdf
11. Zhuang, Y. (2024, 11 de febrero). Imran Khan's 'Victory Speech' from jail shows A.I.'s peril and promise. The New York Times. https://www.nytimes.com/2024/02/11/world/asia/imran-khan-artificial-intelligence-pakistan.html

Informes de política pública global sobre IA

La iniciativa Informes de política pública global sobre IA es un esfuerzo conjunto de IVADO, el principal consorcio canadiense de investigación y movilización de conocimientos sobre IA de la Université de Montréal, y l'Initiative IA+Société de la Université d'Ottawa, cuyo objetivo es proporcionar a los responsables políticos recomendaciones políticas basadas en pruebas para hacer frente a los principales retos mundiales actuales de la IA.

Para esta primera entrega, los profesores Catherine Régis y Florian Martin-Bariteau reunieron a un grupo de destacados expertos en IA de renombre mundial con el fin de desarrollar una guía política de orientación global sobre el impacto de la IA en la democracia y la integridad electoral. El informe se elaboró tras un retiro de una semana organizado por la Società Italiana per l'Organizzazione Internazionale (SIOI) en Roma, Italia, en diciembre de 2024. Fue redactado con el apoyo de Réjean Roy, director de Movilización del Conocimiento, IVADO.

Este proyecto se ha llevado a cabo gracias a la contribución del Fonds de recherche du Québec, del CEIMIA, de la Chaire Canada-CIFAR en IA et droits de la personne del Mila, y de la Chaire de recherche de l'Université d'Ottawa en technologie et société, y con la ayuda de la Délégation du Québec à Rome y la SIOI para la organización del retiro.

Las opiniones expresadas en este documento son responsabilidad exclusiva de los autores.

Catherine Régis es profesora de Derecho de la Université de Montréal y directora de Innovación Social y Política Internacional de IVADO. Experta en gobernanza de la IA, codirige el programa de investigación del Institut canadien de la sécurité de l'IA y es titular de la Cátedra Canadá-CIFAR de IA y Derechos Humanos, Mila.

Florian Martin-Bariteau es catedrático de Investigación Universitaria en Tecnología y Sociedad y profesor asociado de Derecho en la Université d'Ottawa, donde dirige l'Initiative IA + Société y el Centre de recherche en droit, technologie et société. Es profesor asociado del Berkman-Klein Center de la Harvard University.

Jake Okechukwu Effoduh, profesor asistente de la Lincoln Alexander School of Law de la Toronto Metropolitan University, está especializado en Derecho de la IA y derechos humanos internacionales. Contribuye al desarrollo de marcos reguladores de la IA en varios países y dirige importantes proyectos de investigación Canadá-África.

Juan David Gutiérrez, profesor asociado de la Universidad de los Andes en Bogotá, estudia las intersecciones entre políticas públicas y tecnologías. Como miembro experto de la Global Partnership on Artificial Intelligence (GPAI), codirige el proyecto de transparencia algorítmica.

Gina Neff es profesora de Inteligencia Artificial Responsable en la Queen Mary University of London y dirige el Minderoo Centre for Technology and Democracy en la University of Cambridge. Sus investigaciones analizan el impacto de los entornos digitales en el trabajo y la vida cotidiana.

Abogado especializado en derecho digital, **Carlos Affonso Pereira de Souza** es profesor en la Universidade do Estado do Rio de Janeiro (UERJ) y dirige el Instituto do Tecnologia e Sociedade do Río de Janeiro. Como profesor de derecho y tecnología, ha contribuido al desarrollo de las leyes brasileñas de Internet y protección de datos.

Célia Zolynski, profesora de Derecho privado en la Université Paris 1 Panthéon-Sorbonne, es especialista en derecho digital y propiedad intelectual. Como coordinadora del Observatoire de l'IA en París 1, se centra en la regulación de la IA y los derechos fundamentales.

Una iniciativa conjunta de

IVADO

uOttawa | Initiative IA + Société AI + Society

Con el apoyo de

Fonds de recherche Québec

CIFAR

ceimia

Esta iniciativa se ha llevado a cabo gracias, en parte, a la financiación del *Fonds d'excellence en recherche Apogée Canada.*