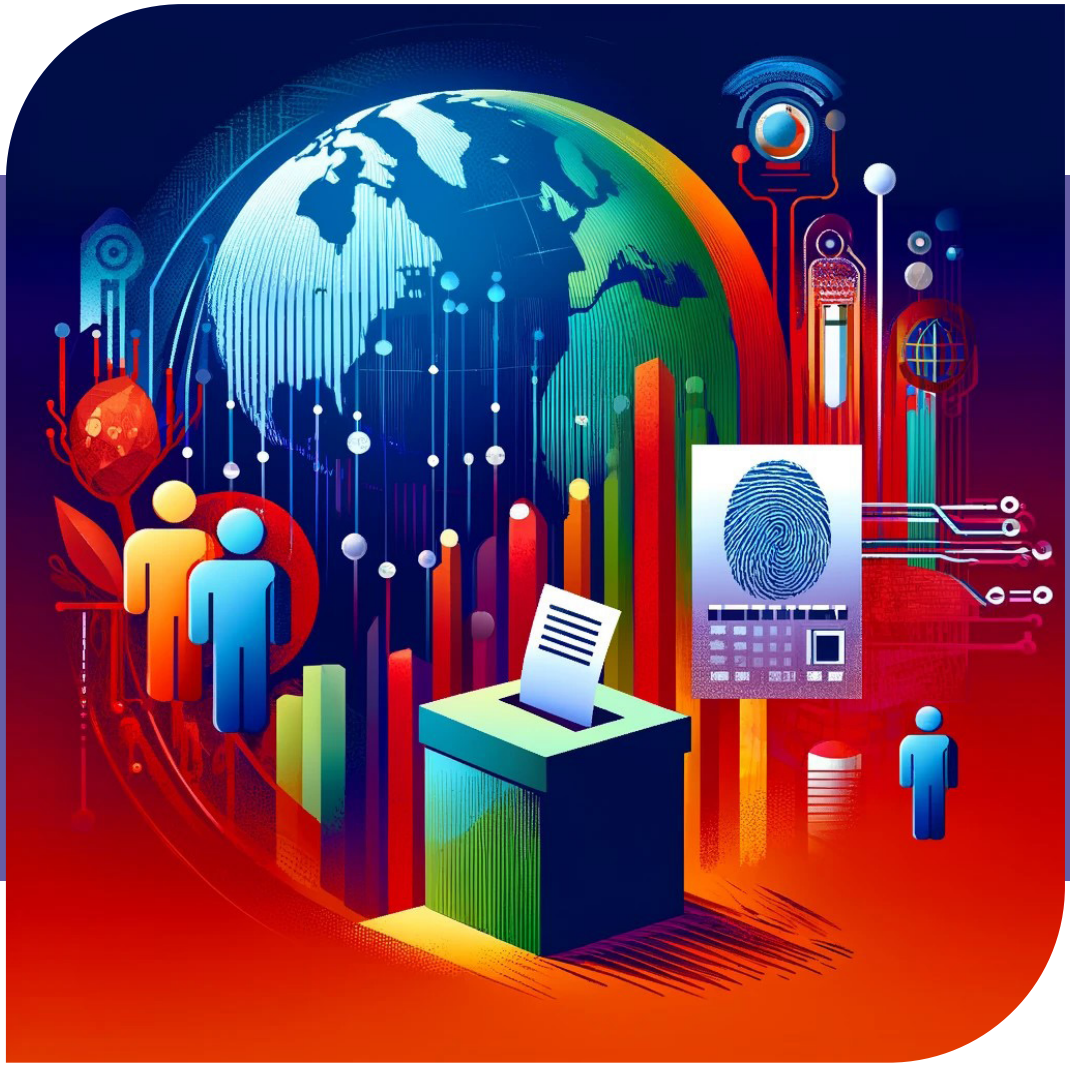
International IDEA

LA INTELIGENCIA ARTIFICIAL PARA LA GESTIÓN ELECTORAL



LA INTELIGENCIA ARTIFICIAL PARA LA GESTIÓN ELECTORAL

Prathm Juneja

IDEA Internacional
Strömsborg
SE-103 34 Estocolmo
SUECIA
+46 8 698 37 00
info@idea.int
www.idea.int

En este informe en ocasiones se utiliza el masculino genérico para referir tanto a hombres como a mujeres, a fin de aligerar el texto.

IDEA Internacional
Strömsborg
SE-103 34 Estocolmo
SUECIA
Teléfono: +46 8 698 37 00
Correo electrónico: info@idea.int
Sitio web: <https://www.idea.int>

Imagen de portada: Generado con DALL E
Diseño: IDEA Internacional
Traducción: Sofie Van Renterghem
Edición: Mariana Enghel

DOI: <https://doi.org/10.31752/idea.2024.89>

ISBN: 978-91-7671-842-1 (versión en pdf)

Lista de siglas y acrónimos

IA	Inteligencia artificial
IAG	Inteligencia artificial generativa
LLM	Modelo de lenguaje de gran tamaño
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OCR	Reconocimiento óptico de caracteres
OMR	Reconocimiento óptico de marcas

Índice

Lista de siglas y acrónimos ..... **iv**
Resumen ejecutivo **1**
Introducción **4**

Capítulo 1
Panorama general: la IA y las elecciones **7**
1.1. Definición de IA 7
1.2. Avances de la IA y su uso en las elecciones 8

Capítulo 2
Oportunidades y desafíos relacionados con el uso de la IA para la gestión electoral **11**
2.1. Introducción 11
2.2. Fase preelectoral 12
2.3. Fase electoral 22
2.4. Fase poselectoral 30
2.5. Retos, riesgos y estrategias de mitigación adicionales 35
2.6. Los caminos a seguir 42

Capítulo 3
El uso de la IA por parte de otros actores políticos y sus efectos en los organismos electorales **44**
3.1. IAG e información falsa 44
3.2. Organizaciones políticas 47
3.3. Amenazas para la seguridad de los sistemas electorales 49
3.4. Los caminos a seguir 51

Capítulo 4
Marcos regulatorios de la IA y su impacto en las elecciones **53**
4.1. Reglamento de Inteligencia Artificial de la Unión Europea 53
4.2. Orden Ejecutiva sobre IA de Estados Unidos 55
4.3. Normativa del Tribunal Superior Electoral de Brasil 56
4.4. Normativa sobre IA en otros países 57

Capítulo 5
Conclusiones **58**

Bibliografía **61**
Anexo A. Términos clave **70**
Sobre el autor **72**
Acerca de IDEA Internacional **73**

RESUMEN EJECUTIVO

Ahora que la inteligencia artificial (IA), y el papel que esta podría desempeñar en las elecciones, se han convertido en un tema que cobra cada vez más importancia, es necesario que los organismos electorales elaboren planes para responder a la IA, así como para utilizarla, en algunos casos, a fin de garantizar elecciones libres, justas y seguras. La IA es un conjunto de tecnologías en rápida evolución que en gran medida carecen de regulación. Además, hasta el momento se ha investigado muy poco su posible impacto en las elecciones.

Es necesario que los organismos electorales elaboren planes para responder a la IA, así como para utilizarla, en algunos casos, a fin de garantizar elecciones libres, justas y seguras.

El objetivo de este informe es brindar apoyo a los organismos electorales y a otros actores interesados a fin de promover una amplia comprensión de las oportunidades, los retos y las implicaciones jurídicas del uso de la IA en las elecciones. Este trabajo se enfoca principalmente en dos temáticas. En primer lugar se ofrece un punto de partida para examinar algunas de las formas en que los organismos electorales podrían utilizar la IA para mejorar la administración de las elecciones, y se examinan los riesgos y las posibles estrategias de mitigación asociadas con esos usos. En segundo lugar se analizan algunas de las formas en que otros actores, además de los organismos electorales, podrían utilizar la IA para influir en los procesos electorales, y se estudian las posibles estrategias de respuesta de dichos organismos. También se describen algunos marcos regulatorios en materia de IA que empiezan a tomar forma en el mundo y se explica cómo podrían afectar el trabajo de los organismos electorales que están considerando ya sea utilizar la IA como parte del proceso electoral o responder al uso que otros actores hacen de estas tecnologías.

Dado que el uso de la IA por parte de los organismos electorales aún es incipiente, en este informe se examinan los ejemplos y los trabajos académicos disponibles hasta el momento sobre el tema y se los relaciona con las perspectivas de otros sectores y otros campos académicos para resaltar las potenciales áreas de uso de la IA en las etapas preelectoral, electoral y poselectoral del ciclo de las elecciones. También se contempla el uso de herramientas de la IA generativa (IAG), como el ChatGPT, por parte del personal de los organismos electorales. En este análisis se considera el uso de la IA para realizar diversas acciones, como la gestión de listas de votantes, el registro de votantes, la planificación de la asignación de recursos, la estimación de los costos electorales, la publicidad dirigida, el seguimiento de las campañas, la biometría y la verificación de votantes, el recuento de los votos y las auditorías poselectorales. Cada uno de estos usos plantea una serie de cuestiones éticas, prácticas y relativas a los derechos humanos, que comprenden aspectos relacionados con la vigilancia, los sesgos, la discriminación, la exactitud, el desempeño, las capacidades técnicas, la ciberseguridad y la confianza pública. En muchos de esos casos, los organismos electorales que estén considerando utilizar la IA podrían mitigar estas preocupaciones mediante rigurosos procesos que garanticen la supervisión humana, el control y la auditoría de los sistemas de IA.

En este informe no se toma una postura respecto de si los organismos electorales deberían o no incorporar el uso de la IA en las elecciones, sino que se presenta una introducción al tema para aquellos organismos electorales que estén considerando posibles usos y se brindan recomendaciones para elaborar normas de aplicación claras, transparentes y respetuosas de los derechos de las personas.

En el informe se aborda una cuestión a menudo discutida, que refiere al uso de la IA por parte de otros actores políticos, entre los que se incluyen los productores de información falsa, las campañas políticas y los piratas informáticos o *hackers*. Si bien la existencia de información falsa sobre las elecciones no es un fenómeno nuevo, los avances de la IAG exacerban los problemas que ya existían pues permiten aumentar la cantidad de información falsa y, en algunos casos, mejorar su calidad. Algunas posibles estrategias para mitigar estos riesgos consisten en garantizar la transparencia, promover la cooperación entre agencias, o desarrollar alianzas con los proveedores y divulgadores de contenidos generados por la IA.

Es probable que durante las campañas políticas se utilice la IA para todo, desde el desarrollo de publicidad dirigida hasta la elaboración de pronósticos electorales, y los organismos electorales deben considerar que estos usos podrían requerir actualizaciones de su mandato y su normativa. La IA también puede incrementar la amenaza de sufrir ciberataques, sobre todo mediante intentos de fraude electrónico de mayor calidad. Por tanto, los organismos electorales deberían considerar la necesidad de fortalecer los protocolos de ciberseguridad existentes para defenderse de estos avances de las capacidades, que provocan un aumento de los riesgos.

Es probable que durante las campañas políticas se utilice la IA para todo, desde el desarrollo de publicidad dirigida hasta la elaboración de pronósticos electorales.

La rápida evolución del entorno regulatorio también puede influir en el papel de la IA en las elecciones. En este informe se ofrece una breve introducción a algunos enfoques regulatorios en materia de IA, entre los que se incluyen el Reglamento de Inteligencia Artificial de la Unión Europea y su enfoque en los sistemas de alto riesgo, la Orden Ejecutiva sobre IA de Estados Unidos y la normativa del Tribunal Superior Electoral de Brasil. En los tres casos, estas normas inciden en las formas en que los organismos electorales podrían utilizar la IA para realizar su trabajo, y podrían repercutir en los mandatos de dichos organismos, sobre todo en lo que se refiere al seguimiento de las campañas políticas.

Si bien todavía hay mucha incertidumbre respecto de cómo los organismos electorales podrían utilizar la IA, y sobre los efectos que tendrán en las elecciones los usos que otros actores hagan de estas tecnologías, es cada vez más imperioso que los organismos electorales empiecen a elaborar planes para adaptarse al nuevo entorno tecnológico. En este informe se ofrece un punto de partida para ese trabajo pues se brinda un panorama general del uso de la IA en las elecciones, que contempla las oportunidades, los retos y las estrategias de mitigación asociadas a su uso por parte tanto de los organismos electorales como de otros actores relevantes.

Es cada vez más imperioso que los organismos electorales empiecen a elaborar planes para adaptarse al nuevo entorno tecnológico.

INTRODUCCIÓN

La conversación sobre la IA y las elecciones se ha centrado principalmente en el papel que la IA podría tener en la generación y la difusión de desinformación.

La inteligencia artificial (IA) constituye un tema cada vez más importante para los organismos electorales y otras organizaciones vinculadas con los procesos electorales. Por lo general gran parte de la conversación sobre la IA y las elecciones se ha centrado principalmente en el papel que la IA podría tener en la generación y la difusión de desinformación[1]. Si bien esta es una temática importante que se aborda en diferentes secciones de este informe, el papel y los efectos potenciales de la IA en las elecciones constituyen un tema mucho más amplio, que abarca desde las formas en que los organismos electorales podrían utilizar la IA durante los procesos electorales hasta las maneras en que otros actores políticos podrían aprovechar la IA para influir en las elecciones.

A fin de contribuir a cerrar esa brecha de conocimiento, en este informe se ofrece un marco para los organismos electorales que estén considerando los usos y los efectos de la IA en las elecciones y en la gestión electoral. Puesto que la IA y las elecciones constituyen un tema amplio que evoluciona rápidamente, en este informe se destacan las áreas que podrían seguir explorando aquellos organismos electorales que están empezando a desarrollar estrategias basadas en la IA en sus contextos específicos.

A pesar de que el tema de los usos de la IA para la gestión electoral ha sido poco investigado hasta el momento, el principal objetivo de este informe es brindar a los organismos electorales un punto de partida —basado en ejemplos tomados de otros campos y

1 La relatora especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión ha definido la desinformación como "la información falaz que se difunde intencionadamente para causar un grave perjuicio social" (Naciones Unidas, 2021, párr.15).

en el examen de los procesos actuales de distintos organismos electorales— para analizar de qué manera el uso de la IA podría contribuir a mejorar la administración de las elecciones. Muchos de los ejemplos que se presentan en este informe sobre el uso actual de la IA por parte de distintos organismos electorales proceden de Estados Unidos, un país que ha tenido muchas oportunidades de utilizar la IA porque cuenta con un sistema electoral federalizado, que a menudo se gestiona a nivel estatal y por condado, y porque hay una gran cantidad de empresas de IA que están activas en ese país.

Como resultado de los avances de la IA se han creado nuevas oportunidades para que los organismos electorales implementen sistemas basados en una mejor lógica y desplieguen capacidades analíticas y generativas con el potencial para mejorar la accesibilidad, optimizar la planificación logística y potenciar el entorno informativo de las elecciones. Estos beneficios potenciales conllevan posibles externalidades negativas en lo que respecta a la ciberseguridad, los derechos humanos y la discriminación, entre otras cuestiones.

Como resultado de los avances de la IA se han creado nuevas oportunidades para los organismos electorales.

Cabe destacar que el objetivo de este informe no es recomendar a los organismos electorales el uso de la IA ni brindar instrucciones para su utilización, sino más bien ofrecer a aquellos organismos electorales interesados en el tema una introducción general a esta cuestión. Otro objetivo del informe es brindar a los organismos electorales un punto de partida para examinar cómo otros actores, como las campañas políticas y los piratas informáticos, podrían utilizar la IA para influir en la gestión y el resultado de las elecciones. En vista de la proliferación de herramientas avanzadas de IA y de lo fácil que es acceder a ellas, los organismos electorales deben empezar a planificar los usos de la IA, y deben considerar la implementación de estrategias de mitigación y el desarrollo de enfoques regulatorios.

El informe está organizado de la siguiente manera. En el capítulo 1 se ofrece una definición del concepto de IA, se presenta una breve reseña histórica de su uso en las elecciones y se analiza cómo los avances recientes de la IA impulsaron la elaboración de este informe. En el capítulo 2 se presenta una lista no exhaustiva de los posibles usos de la IA por parte de los organismos electorales a lo largo del ciclo electoral, y se detallan los pasos a seguir para su implementación, los riesgos asociados con los diferentes usos y las posibles medidas de mitigación. En el capítulo 3 se analiza un aspecto diferente pero importante para los organismos electorales, a saber: cómo otros actores políticos podrían utilizar la IA para

influir en la gestión electoral, y para qué tipo de escenarios deberían empezar a prepararse los organismos electorales a corto plazo. Por último, en el capítulo 4 se examinan algunos de los enfoques globales y nacionales desarrollados para regular el uso de la IA, especialmente en lo que respecta a los organismos públicos, y se analiza cómo estas normativas podrían determinar el uso de la IA por parte de los organismos electorales y su respuesta a estas tecnologías.

Capítulo 1

PANORAMA GENERAL: LA IA Y LAS ELECCIONES

1.1. **DEFINICIÓN DE IA**

En este informe se considera la definición de sistemas de IA proporcionada por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), que es ampliamente aceptada:

> Un sistema de IA es un sistema basado en máquinas que, para objetivos explícitos o implícitos, infiere, a partir de los datos de entrada que recibe, cómo generar información de salida como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos reales o virtuales. Una vez implementados, los distintos sistemas de IA presentan diversos niveles de autonomía y varían en su capacidad de adaptación (OCDE, 2019).

Esta definición comprende a los métodos estadísticos tradicionales, como las regresiones lineales y la comparación probabilística de patrones, así como a las técnicas modernas de aprendizaje automatizado (*machine learning*), como las redes neuronales, siempre que se utilicen para desarrollar resultados de salida que puedan influir en entornos físicos o virtuales. A partir de esta definición, en este informe se utiliza el término IA para abarcar una amplia gama de sistemas, y se usan términos más específicos para describir las tecnologías subyacentes. Más información sobre los términos utilizados puede consultarse en el anexo A.

1.2. **AVANCES DE LA IA Y SU USO EN LAS ELECCIONES**

La IA se ha utilizado para la gestión electoral por mucho tiempo. En Estados Unidos, por ejemplo, el Centro de Información de Registro Electrónico trabaja con un consorcio de Estados para analizar el registro de votantes, el registro de vehículos y otros registros oficiales con el fin de contribuir al mantenimiento del padrón electoral. El *software* del Centro de Información de Registro Electrónico se basa en el aprendizaje automatizado (*machine learning*) y genera recomendaciones para el funcionariado electoral estatal sobre los votantes que es probable que hayan sido registrados dos veces y sobre los votantes elegibles no registrados (Centro de Información de Registro Electrónico, 2024). Los sistemas de verificación biométrica, ya sea en uso o en fase de prueba en muchos países, suelen ser ejemplos de IA que utiliza modelos de aprendizaje profundo para comparar datos biométricos con conjuntos de datos existentes (Wolf et al., 2017). Las herramientas de comparación de firmas, que también se utilizan ampliamente en Estados Unidos, constituyen un ejemplo de IA (Bender, 2022). Los países que utilizan técnicas basadas en modelos estadísticos para la asignación de recursos, la localización de los centros de votación, las campañas publicitarias o el análisis de los resultados electorales también podrían estar haciendo uso de diversas formas de IA.

Aunque pocas veces se lo reconozca, la IA no es algo nuevo para las elecciones ni para las personas encargadas de su administración. Los avances en el desarrollo, el despliegue y la comercialización de la IA han incrementado tanto las oportunidades como los compromisos que conlleva su uso en las elecciones.

Las primeras investigaciones sobre lo que hoy se considera como IA probablemente comenzaron entre principios y mediados del siglo XX, con el test de Turing y los primeros conceptos sobre las redes neuronales artificiales. Los primeros avances en materia de IA se centraron sobre todo en la tarea específica de diseñar los denominados sistemas expertos o modelos diseñados para imitar a personas expertas en determinados ámbitos, y muchos de los primeros desarrollos de la IA se enfocaron en la toma de decisiones para juegos. Hasta hace poco la mayoría de los avances de la IA correspondían a esos sistemas más limitados y los modelos tenían un funcionamiento más parecido al de la estadística tradicional, es decir, tomaban datos de entrada específicos y desarrollaban fórmulas interpretables para determinar la producción de datos

de salida, lejos de las abstracciones que hoy se asocian con los enfoques de aprendizaje profundo.

La era actual de la IA ha sido impulsada en gran medida por los avances del aprendizaje profundo, entre los que se incluye la arquitectura de transformadores (Vaswani et al., 2017). Junto con la creciente disponibilidad de grandes conjuntos de datos y la cada vez mayor capacidad de procesamiento informático, estas innovaciones han posibilitado que los modelos de aprendizaje profundo tomen grandes cantidades de datos no estructurados, como texto, imágenes y video, y los utilicen para entrenar modelos generalizados. Los avances del aprendizaje por transferencia han permitido a los desarrolladores especializar estos modelos más amplios para que sean usados en una variedad de ámbitos y disciplinas, como la medicina, la ciencia, los medios de comunicación y, cada vez más, la política. A pesar de que los enfoques de aprendizaje profundo han permitido mejorar en gran medida el desempeño de muchas tareas, especialmente en lo que respecta a la modelización de los idiomas, estos avances a menudo conllevan una desventaja que es la falta de interpretabilidad, que se debe a los niveles de abstracción inherentes a las redes neuronales profundas. Mientras que las regresiones tradicionales ofrecen fórmulas claras sobre cómo los datos de entrada se convierten en datos de salida, en las redes neuronales profundas no resulta tan claro cómo y por qué determinados datos de entrada dan lugar a ciertos resultados.

Estos avances más recientes son los que han impulsado la elaboración de este informe y los que están creando nuevas oportunidades y preocupaciones para las autoridades electorales. Los modelos de lenguaje de gran tamaño (LLM) ofrecen a los organismos electorales y a los actores políticos la posibilidad de analizar, generar y resumir textos complejos. Otros modelos de IA generativa (IAG) ofrecen capacidades similares para otros tipos de resultados de salida, como video, audio y datos numéricos. Los avances de técnicas como las redes neuronales gráficas o los métodos de *boosting*[2] y *bagging*[3] abren nuevas vías para el análisis de redes y de conjuntos de datos complejos. En el siguiente capítulo se analizan diferentes formas en que los organismos electorales podrían utilizar los sistemas de IA para mejorar la administración de

2 El término *boosting* refiere a un metaalgoritmo de aprendizaje automático que reduce el sesgo y la varianza en un contexto de aprendizaje supervisado.

3 El término *bagging* (o "embolsado") refiere a un metaalgoritmo de aprendizaje automatizado diseñado para mejorar la estabilidad y precisión de algoritmos de aprendizaje (*machine learning*) usados en tareas de clasificación estadística y regresión.

las elecciones. Más adelante también se analiza de qué forma el uso de la IA por parte de otros actores podría afectar a los organismos electorales.

Muchos países están elaborando normativas para regular el uso de la IA.

Cabe destacar que en todo el mundo hay organismos gubernamentales y empresas que ya están realizando distintos tipos de pruebas con relación a estos avances de la IA, y muchos países están elaborando normativas para regular el uso de la IA (Carrasco et al., 2024). Es probable que estas estrategias más amplias del sector público basadas en la IA influyan en los recursos y las capacidades a los que tendrán acceso los organismos electorales a la hora de utilizar la IA para la gestión electoral.

Capítulo 2

OPORTUNIDADES Y DESAFÍOS RELACIONADOS CON EL USO DE LA IA PARA LA GESTIÓN ELECTORAL

2.1. **INTRODUCCIÓN**

En este capítulo se presenta una lista no exhaustiva de los posibles usos de la IA por parte de los organismos electorales durante las elecciones en las fases preelectoral, electoral y poselectoral del ciclo de elecciones, a pesar de que algunos usos podrían extenderse durante todo el ciclo electoral. Muchos de estos usos no han sido probados y se basan en experiencias de trabajo de la industria y de otros ámbitos académicos. También se hace referencia al caso de los organismos electorales que han incorporado en su trabajo cotidiano herramientas de la IAG de uso general, como Microsoft Copilot.

Al examinar cada caso de uso de la IA se los desafíos éticos y prácticos, así como los desafíos en términos de derechos humanos, asociados con su aplicación. Al final también se incluye una lista general de retos adicionales asociados con el uso de sistemas basados en IA por parte de los organismos electorales, y se examinan posibles estrategias para mitigar algunos de los riesgos identificados. El capítulo concluye con un resumen de una serie de recomendaciones dirigidas a los organismos electorales que estén considerando la posibilidad de utilizar la IA para la gestión electoral.

2.2. **FASE PREELECTORAL**

La fase preelectoral es la parte del ciclo electoral en que la atención se centra principalmente en la planificación, la capacitación, el intercambio de información y las tareas de registro.

2.2.1. **Registro y elegibilidad de votantes**

La gestión de la lista de votantes, o el proceso de limpieza y auditoría del padrón electoral, es una tarea que podría verse favorecida en buena medida por los modelos de la IA.

Gestión de la lista de votantes

Caso de uso de la IA. La gestión de la lista de votantes, o el proceso de limpieza y auditoría del padrón electoral, es una tarea que podría verse favorecida en buena medida por los modelos de IA. Muchos países, por ejemplo Indonesia (Akbar et al., 2021), ya están utilizando enfoques simples de comparación de patrones para detectar y señalar registros duplicados, y están usando herramientas de filtrado para buscar datos faltantes, incompletos o incorrectos. Los modelos más avanzados de comparación de datos pueden ser útiles para identificar registros repetidos al sugerir la probabilidad de que varios registros se refieran a la misma persona. Los modelos pueden comparar la información de los registros con otras fuentes de documentación oficial o con datos históricos y recomendar que se haga una investigación más exhaustiva de determinados registros.

Implementación. Para administrar las listas de votantes suelen utilizarse enfoques algorítmicos, pero en algunos casos se han empleado métodos de aprendizaje automático más avanzados. El Centro de Información de Registro Electrónico de Estados Unidos utiliza el aprendizaje centrado en entidades para comparar diversos registros, como los datos de la seguridad social, los registros de cambios de domicilio, los registros de votantes y los datos del registro automotor (Centro de Información de Registro Electrónico, 2024).

Riesgos. El uso de cualquier enfoque algorítmico para la administración de listas de votantes genera reparos, especialmente si se trata de enfoques de IA no interpretables que se utilizan sin supervisión humana (Deepak, Simoes y MacCarthaigh, 2023). Los modelos inexactos —tanto los enfoques tradicionales de comparación de patrones como los modelos más avanzados de aprendizaje profundo— conllevan el riesgo de privar del derecho al voto a votantes elegibles y podrían generar resultados discriminatorios debido a las diferencias en las distribuciones de nombres y direcciones. La falta de transparencia podría acrecentar los riesgos en lo que respecta a la integridad electoral. Existen

pruebas de que el uso de Crosscheck, una herramienta para la gestión de listas de votantes que se ha utilizado en Estados Unidos, conllevó el riesgo de eliminar por error como mínimo a unos 300 votantes elegibles para evitar un voto doble (Goel et al., 2020). Algunos de estos riesgos podrían atenuarse si los organismos electorales considerasen el uso de enfoques algorítmicos para la gestión de listas solamente como parte de un proceso más exhaustivo dirigido por personas, es decir, como un punto de partida para las investigaciones.

Registro e identificación de votantes

Caso de uso de la IA. Uno de los objetivos del proceso de registro de votantes es hacer una comprobación previa de la elegibilidad de una persona para votar, a fin de que, cuando el votante presente su papeleta, solo sea preciso verificar su identidad. En las jurisdicciones en que el registro de votantes activos constituye un requisito, este proceso en general requiere que los votantes presenten algún tipo de identificación oficial, una prueba de elegibilidad y posiblemente datos biométricos, como huellas dactilares, imágenes faciales o una firma. Los modelos de IA preparados para comparar documentos de identificación o datos biométricos pueden ser útiles para acelerar y posiblemente mejorar la exactitud de este proceso, así como para evitar la duplicación de registros. La IA ofrece nuevas formas de identificación biométrica de los votantes en los centros de votación, como la identificación facial o de huellas dactilares, que permiten a un modelo comparar los datos biométricos de un votante con los datos biométricos registrados en el padrón electoral.

Implementación. En muchos casos, las herramientas biométricas se basan en la IA y usan modelos de aprendizaje profundo para comparar *hashes* biométricos (es decir, representaciones numéricas de datos biométricos como las huellas dactilares). El uso de un sistema biométrico para el registro de los votantes brinda a los organismos electorales la posibilidad de volver a verificar los datos biométricos en los centros de votación o de incluirlos en las tarjetas de identificación de los votantes. En 2016 el 35 por ciento de los organismos electorales encuestados consideraban datos biométricos como parte de su proceso de registro (Wolf et al., 2017). India, que cuenta con un sistema general de identificación biométrica que incluye datos sobre el iris, las huellas dactilares y el rostro de las personas, está examinando la posibilidad de utilizar estos datos para identificar a los votantes (Livemint, 2022).

Riesgos. Cabe señalar que en las jurisdicciones en que el fraude electoral es extremadamente raro la implementación de estrictos métodos de verificación podría contribuir escasamente a mejorar la seguridad electoral y, en cambio, podría privar injustamente de sus derechos a votantes legítimos (Deepak, Simoes y MacCarthaigh, 2023). La exactitud de las herramientas de comparación de firmas podría ser tan solo del 74,3 por ciento y su uso, por tanto, podría privar del derecho al voto a votantes elegibles (Hussain et al., 2015). Además, aunque a menudo las tasas de error de los sistemas biométricos son bajas, cuando estos sistemas fallan pueden afectar en mayor medida a las personas afrodescendientes, lo que constituiría una privación de derechos discriminatoria (Deepak, Simoes y MacCarthaigh, 2023; Wolf et al., 2017). La biometría conlleva una serie de graves riesgos relativos a la seguridad y la privacidad de los datos que, además de constituir problemas en sí mismos, pueden disuadir de participar en las elecciones a aquellas personas preocupadas por la privacidad o a los votantes históricamente discriminados (Wolf et al., 2017). Para reducir estos riesgos los organismos electorales podrían ofrecer alternativas a la comprobación biométrica previa o crear procesos claros y fácilmente accesibles para apelar las decisiones de los sistemas biométricos.

2.2.2. **Planificación**

Los modelos y las simulaciones de la IA pueden ser útiles para optimizar el proceso de planificación preelectoral.

Ubicación de los centros de votación y asignación de recursos

Caso de uso de la IA. Un elemento clave del proceso de planificación preelectoral consiste en decidir cómo asignar los recursos electorales, lo que incluye determinar la ubicación de los centros de votación, definir el número de cabinas de votación y establecer el número de trabajadores electorales que se desempeñarán en cada uno de los centros de votación. Contar con una estimación exacta de los recursos necesarios permite que los procesos electorales sean más accesibles, rápidos y sencillos para los votantes. Los modelos y las simulaciones de la IA pueden ser útiles para optimizar el proceso de planificación preelectoral, y en algunos casos podrían tornarlo más imparcial al predecir la popularidad de los recintos electorales y minimizar la distancia entre los votantes y los respectivos centros de votación. Los modelos también podrían ser útiles para estimar dónde es más necesaria la presencia de personal electoral. El uso de estos modelos podría ser útil para mejorar el acceso a los centros de votación, lo que podría incidir favorablemente en los índices de participación electoral.

Implementación. Como señalan Deepak, Simoes y MacCarthaigh (2023), si bien hay pocas pruebas de que se esté utilizando la IA para seleccionar la ubicación de los centros de votación, otras industrias están utilizando la IA para optimizar la ubicación de sus instalaciones (Al-Haidary et al., 2021). Las herramientas para planificar y determinar la asignación de empleados basadas en la IA podrían ser útiles para asignar personal a diferentes centros de votación (Talarico y Maya Duque, 2015). Los modelos construidos internamente para estos fines podrían utilizar algoritmos supervisados, basados en escenarios "ideales", para seleccionar los centros de votación y asignar recursos con base en datos históricos, o en algoritmos no supervisados, orientados a optimizar la distancia o la eficiencia.

Riesgos. Cuando se evalúa el uso de la IA para seleccionar la ubicación de los centros de votación la ausencia de matices en los datos disponibles para los modelos constituye un gran motivo de preocupación (por ejemplo, mientras que un funcionario electoral puede contemplar cuestiones relacionadas con la accesibilidad o la seguridad de un lugar específico, los modelos pueden pasar por alto esos matices). También es posible que los conjuntos de datos carezcan de suficiente información sobre factores que han demostrado tener un impacto en las tasas de participación, como la accesibilidad, la importancia de la comunidad, o la visibilidad y la calidad del interior del recinto (Mann y Stein, 2019). Los algoritmos destinados a optimizar constantemente la ubicación de los centros de votación podrían incrementar el costo de las acciones dirigidas a informar sobre los nuevos lugares, y la volatilidad podría confundir a los votantes y disminuir las tasas de participación (Deepak, Simoes y MacCarthaigh, 2023). A pesar de ser importante, la supervisión humana también podría resultar difícil en este caso, ya que los cambios manuales, como el traslado de un recinto electoral, podrían afectar los cálculos del modelo y comprometer aún más la imparcialidad. La optimización basada en variables específicas, como la distancia general desde un centro de votación, podría generar la discriminación de determinadas categorías de votantes, por ejemplo, de aquellos que residen en zonas rurales. La asignación general de recursos, con relación tanto a las cabinas de votación como al personal electoral, también despierta importantes preocupaciones similares (Kwon, Moreno y Raman, 2023).

Definición de la estimación de la línea de base

Caso de uso de la IA. En algunos casos, dependiendo de su mandato, un organismo electoral podría tener interés en desarrollar

un conjunto de previsiones relacionadas con diversos aspectos de las elecciones, como la recaudación de fondos para la campaña, los gastos de campaña, los índices de participación electoral e incluso los resultados de las elecciones. En todos los casos estas estimaciones podrían constituir una línea de base útil para la detección de anomalías durante o después de las elecciones. Por ejemplo, los cálculos sobre la recaudación de fondos para la campaña pueden ser útiles para que los organismos electorales hagan un mejor seguimiento de los gastos de campaña, las solicitudes de auditoría y la contratación de espacios en los medios de comunicación. Las predicciones sobre los índices de participación electoral pueden contribuir a que los organismos electorales hagan una mejor estimación de cuáles serán las necesidades en materia de logística, como la asignación de boletas antes de las elecciones o el recuento de estas después de la votación. Las técnicas estadísticas tradicionales, como las regresiones, y los modelos de IA más avanzados podrían ser de utilidad para desarrollar estos procesos.

Implementación. Tal vez la principal estimación de una línea de base que podría ser útil para otras áreas de trabajo de los organismos electorales consista en el uso de técnicas de la IA o de la ciencia de datos para predecir los índices de participación electoral. A tal fin los organismos electorales podrían considerar el uso de métodos tradicionales empleados por académicos y agencias de encuestas, o el uso de métodos más avanzados, como el algoritmo de bosque aleatorio (*random forest*) o el *boosting* (Moses y Box-Steffensmeier, 2021; Kennedy, Wojcik y Lazer, 2017). Otros métodos similares también podrían ser útiles para predecir los gastos de campaña y las tendencias de la recaudación de fondos, y de hecho existen investigaciones que examinan el uso de diversos métodos para realizar tareas similares en los ámbitos de la inversión, la microfinanciación colectiva y diversas actividades sin fines de lucro (Liu y Hu, 2024). En el ámbito político se ha registrado un incremento del número de nuevas empresas que intentan vender a las campañas políticas herramientas de aprendizaje automático para hacer predicciones sobre la participación electoral y la recaudación de fondos (Markay, 2022). Las grandes diferencias entre los resultados estimados y los reales podrían ser de utilidad para el desarrollo de nuevas y más exhaustivas investigaciones.

Riesgos. El principal riesgo que plantea el uso de la IA para estimar líneas de base es la alta probabilidad de que las técnicas de modelización arrojen resultados inexactos. Diversos factores influyen en las estadísticas sobre participación electoral y recaudación de

fondos de campaña, y muchos de ellos no se miden. Por tanto, es baja la probabilidad de que la IA y los métodos estadísticos tradicionales generen estimaciones lo suficientemente confiables como para que los organismos electorales puedan utilizarlas y sea para tomar buenas decisiones o como línea de base de ejercicios de comparación, excepto en los casos en que las predicciones difieran drásticamente de la realidad. La falta de exactitud podría incidir en la toma de decisiones de los organismos electorales y afectar la imparcialidad del proceso de auditoría. El uso de predicciones de cualquier tipo por parte de los organismos electorales podría comprometer la integridad electoral. Estos modelos conllevan un riesgo significativo en lo que respecta a la integridad electoral, las actividades de campaña y la confianza pública debido a la posibilidad de que se produzca una filtración de información. Los organismos electorales que estén considerando la implementación de la IA para estos fines podrían minimizar los riesgos mediante el desarrollo de prácticas de ciberseguridad estrictas, y por medio de pruebas piloto y comparaciones exhaustivas de los nuevos modelos, a fin de comprobar su confiabilidad.

Proyección de los costos electorales

Caso de uso de la IA. Para los organismos electorales puede ser de utilidad contar con una proyección del costo administrativo de las elecciones como parte de su proceso presupuestario. En vista de que las elecciones tienen muchos costos variables, que van desde la compra de máquinas de votación y de boletas hasta la contratación de personal electoral, la IA puede ser útil para estimar mejor cuántos equipos, personas y recursos se necesitarán. Muchos organismos electorales ya realizan proyecciones aproximadas con fines presupuestarios, y a menudo basan sus estimaciones en el peor escenario posible relativo a las elecciones anteriores, pero la IA podría proporcionar estimaciones más exactas. Al igual que ocurre con relación a la asignación de recursos y la estimación de líneas de base, los modelos de IA pueden producir proyecciones aproximadas de diversos costos, como aquellos relacionados con la seguridad electoral, las máquinas de votación, la contratación de personal o la compra de boletas, entre otros.

Para los organismos electorales puede ser de utilidad contar con una proyección del costo administrativo de las elecciones como parte de su proceso presupuestario.

Implementación. Se han realizado pocas investigaciones sobre los costos de la gestión electoral y no ha sido posible encontrar ningún trabajo en que se utilice la IA para estimar dichos costos (Clark, 2019). Sin embargo, algunas investigaciones han examinado el papel que los algoritmos de aprendizaje profundo pueden desempeñar para mejorar las estrategias presupuestarias de los gobiernos, al

utilizar los gastos potenciales como datos de entrada para optimizar determinados resultados de salida (Valle-Cruz, Fernández-Cortez y Gil-García, 2022). Los avances relativos al uso del aprendizaje automático en ámbitos como la predicción de riesgos o la fijación de precios de los seguros pueden constituir un punto de partida útil (Kan et al., 2019).

Riesgos. Dada la falta de investigaciones centradas en el estudio de métodos para proyectar los costos de las elecciones, la principal preocupación relativa al uso de la IA para este fin es la exactitud. El riesgo de los modelos que tienen un bajo nivel de exactitud, especialmente de aquellos en los que se confía para tomar decisiones, es que los organismos electorales no estén suficientemente preparados para las elecciones, lo que a su vez podría afectar en gran medida la integridad electoral. Para mitigar estos riesgos los organismos electorales podrían desarrollar proyecciones piloto basadas en la IA para comprobar su nivel de exactitud en comparación con los resultados de los métodos tradicionales.

Los LLM pueden ser útiles para detectar publicaciones en las redes sociales sobre actos de violencia planificados o potenciales en distintos centros de votación.

Predicción de la seguridad y la violencia electoral

Caso de uso de la IA. Para garantizar la seguridad e integridad de las elecciones, identificar de forma anticipada los lugares donde podrían ocurrir actos de violencia electoral puede ser de gran utilidad para los organismos electorales y las fuerzas de seguridad. Tal como se ha señalado en las secciones anteriores con relación a otros aspectos de la gestión electoral, los modelos entrenados con datos sobre zonas donde se ha producido violencia anteriormente o con datos sobre zonas relacionadas con hechos de violencia pueden ayudar a los organismos electorales a decidir dónde es prioritaria la presencia de los servicios de seguridad. Asimismo, los LLM pueden ser útiles para detectar publicaciones en las redes sociales sobre actos de violencia planificados o potenciales en distintos centros de votación. Si se los combina, estos modelos pueden ayudar a los organismos electorales a identificar anticipadamente los lugares de votación de alto riesgo, a fin de evitar que se produzcan actos de violencia.

Implementación. Los modelos supervisados entrenados con datos sobre centros de votación o zonas geográficas donde se produjo violencia electoral anteriormente pueden ser útiles para predecir dónde ocurrirán hechos de violencia en el futuro (Deepak, Simoes y MacCarthaigh, 2023). Los LLM adecuadamente ajustados que se aplican a publicaciones en las redes sociales pueden ser útiles para alertar sobre posibles amenazas de violencia o para identificar zonas

específicas que estén recibiendo excesiva atención por parte de grupos violentos. Aunque es limitado el trabajo que se ha realizado con relación a los centros de votación en particular, la IA se está utilizando desde hace tiempo para la vigilancia policial predictiva, y muchos gobiernos y empresas privadas están desarrollando herramientas con este fin (Hardyns y Rummens, 2018).

Riesgos. Las acciones que conforman la vigilancia policial predictiva son muy controvertidas, ya que plantean graves preocupaciones éticas y en términos de derechos humanos debido a que pueden carecer de exactitud y generar actos de discriminación. Hay evidencia que señala que, debido a la falta de datos de alta calidad, a los sesgos existentes y a la imposibilidad de interpretar la mayoría de los algoritmos de aprendizaje profundo, dichos sistemas perpetúan las desigualdades sistémicas de la actuación policial, mientras que no existen pruebas sólidas de su eficacia (Gstrein, Bunnik y Zwitter, 2019; Richardson, Schultz y Crawford, 2019). Existen pocas pruebas de que la vigilancia policial predictiva produzca resultados efectivos, pero hay muchos documentos en que se describe su potencial para incrementar el número de violaciones de los derechos civiles y humanos (Van Brakel, 2016). Una mayor presencia policial en los centros de votación podría reducir los índices de participación electoral, influir en los resultados de las elecciones y reducir la confianza en el proceso electoral (Deepak, Simoes y MacCarthaigh, 2023).

2.2.3. **Educación cívica y movilización de los votantes**

Compartir información electoral

Caso de uso de la IA. La IA, y en especial los LLM, pueden ser útiles para adaptar la información electoral a subgrupos específicos de la población. Dado que muchos organismos electorales tienen el mandato de mejorar la equidad y el acceso a la votación, usar diversas estrategias de comunicación para informar a diferentes subgrupos de la población podría constituir una forma de garantizar un acceso igualitario a la información. Esto es especialmente pertinente para garantizar el acceso a la información de aquellos votantes que cuentan con conocimientos técnicos limitados, ya que la IA se puede utilizar para desarrollar formas de presentar la información electoral que faciliten una comprensión intuitiva. Por ejemplo, los *chatbots*[4] basados en LLM y entrenados a partir de información proveniente de los organismos electorales y de

4 Programas informáticos con los que se puede mantener una conversación.

las preguntas frecuentes que estos reciben pueden constituir una herramienta útil para que los organismos electorales brinden información en un formato adaptado a las consultas específicas de los votantes, que sea fácil de usar y no requiera navegar manualmente por los sitios web electorales (Eisen et al., 2023).

Implementación. Algunas investigaciones se han centrado en el desarrollo de una arquitectura de *chatbot* para mejorar el acceso a la información electoral de las personas mayores y de las personas que votan por primera vez —se trata de un *chatbot* entrenado específicamente con base en las preguntas más frecuentes dirigidas a los organismos electorales (Muppasani et al., 2023)—. Cabe señalar que los organismos electorales deben ser cuidadosos si deciden utilizar *chatbots* y deben asegurarse de utilizar tecnologías de bucle cerrado, como la generación aumentada por recuperación, a fin de garantizar que el LLM solo utilice información predefinida para responder a las consultas.

Riesgos. El uso de *chatbots* basados en LLM para la gestión electoral suscita serias preocupaciones acerca de la validez de la información, por lo que los organismos electorales tendrán que realizar pruebas y auditorías exhaustivas para evitar alucinaciones de los LLM y prevenir la difusión de información falsa (Rawte, Sheth y Das, 2023). Es preciso realizar auditorías de seguridad para evitar que actores malintencionados vulneren los LLM y filtren datos o compartan información incorrecta (Wei, Haghtalab y Steinhardt, 2023). Incluso si la probabilidad de errores es baja, es probable que cualquier tipo de información falsa compartida por un *chatbot* autorizado por un organismo electoral genere controversia y afecte la integridad de las elecciones. Para mitigar estos riesgos los organismos electorales pueden realizar pruebas y auditorías exhaustivas, y asegurarse de utilizar modelos con probabilidades de alucinación limitadas.

Los organismos electorales que tienen el mandato de incrementar los índices de participación electoral o de distribuir información electoral entre distintos grupos de la población pueden beneficiarse del uso de la IA para crear campañas publicitarias dirigidas.

Publicidad dirigida

Caso de uso de la IA. Los organismos electorales que tienen el mandato de incrementar los índices de participación electoral o de distribuir información electoral entre distintos grupos de la población pueden beneficiarse del uso de la IA para crear campañas publicitarias dirigidas. La publicidad dirigida puede resultar útil para mejorar el acceso a la información de personas que habitualmente no participan en los procesos electorales. Los modelos de IAG podrían utilizarse para automatizar el proceso de creación o elaboración del primer borrador de material publicitario dirigido a grupos específicos de la población. La IA, y en especial los modelos

no supervisados, como los modelos de agrupamiento, pueden ser útiles para identificar a los grupos que históricamente han sido desatendidos en las comunicaciones de los organismos electorales.

Implementación. La mayor parte de los trabajos que analizan el papel de la IAG en la movilización de los votantes se centran en la función que esta puede desempeñar en la publicidad política dirigida vinculada a las campañas electorales y sus organizaciones afiliadas. Los resultados de algunos estudios señalan que el uso de herramientas de la IAG para adaptar los anuncios en función de los rasgos de personalidad del público objetivo generó incrementos de la participación (Simchon, Edwards y Lewandowsky, 2024). A su vez, en trabajos previos centrados en el estudio de anuncios de Facebook para audiencias microsegmentadas se observó un impacto en los índices de participación solo en el caso de elecciones estadounidenses altamente competitivas (Haenschen, 2022). La implementación requeriría suministrar datos sobre los usuarios (generalmente provenientes de empresas de redes sociales) a las herramientas de la IAG para generar publicidad dirigida a subgrupos de la base de usuarios.

Riesgos. La publicidad para audiencias microsegmentadas, especialmente impulsada por la IAG, plantea serias preocupaciones en cuanto a la privacidad, la manipulación y la exactitud de los datos. Es posible que a los votantes les incomode que sus datos personales sean utilizados para impulsarlos a votar, mientras que las acciones exitosas podrían crear desigualdades en el proceso electoral y poner en tela de juicio la integridad electoral. Los sistemas completamente automatizados pueden provocar alucinaciones de las herramientas de la IAG, pueden ocasionar que se comparta información incorrecta sobre las elecciones o pueden estar sesgados políticamente. Además, tanto el proceso de selección de audiencias microsegmentadas como las plataformas utilizadas para difundir esos anuncios generan reparos por la posible creación de desigualdades, ya que los organismos electorales podrían dirigirse de forma desproporcionada a determinados subgrupos de la población (Ali et al., 2019). La potencial utilidad de estas herramientas aún no se ha investigado lo suficiente y es posible que su uso no tenga un impacto significativo en los índices de participación en comparación con los efectos de estrategias más generales dirigidas a la movilización de votantes, lo que podría generar reparos en cuanto a la proporcionalidad de las acciones.

2.3. **FASE ELECTORAL**

La fase electoral es la parte del ciclo electoral en que la atención se centra principalmente en la campaña, la votación, y el seguimiento y la tabulación de los resultados.

2.3.1. **Seguimiento de campañas y medios de comunicación**

Seguimiento de la información falsa en redes sociales

Caso de uso de la IA. Un posible caso de uso de la IA para los organismos electorales consiste en la utilización de LLM y de redes neuronales gráficas en las plataformas de las redes sociales para detectar y resumir la información falsa habitual sobre las elecciones. Los LLM permiten detectar tendencias en la información falsa y alertar sobre los casos que despiertan más preocupación, como categorías de mensajes con información engañosa sobre la hora o el lugar en que se desarrollarán las elecciones o sobre la elegibilidad de determinados votantes. Los modelos también pueden ser útiles para detectar mensajes específicos que infringen las leyes electorales. Esto puede brindar a los organismos electorales la oportunidad de elaborar planes para responder de forma más fácil y más rápida, en comparación con las posibilidades que ofrece el seguimiento manual de las plataformas de las redes sociales, lo que constituye un elemento clave para reducir el impacto de la información falsa en las elecciones. La amenaza que supone la información electoral falsa en las redes sociales se examina más detenidamente en el capítulo 3.

Implementación. En una cantidad considerable de investigaciones se ha examinado el uso de los LLM para detectar o resumir tendencias en relación con la información falsa. Además, diversas empresas privadas y organizaciones sin fines de lucro están desarrollando herramientas para la realización de esta tarea (Kondamudi et al., 2023; Dhiman et al., 2023). La implementación de estas herramientas requerirá una planificación cuidadosa a fin de considerar la información sobre el contexto específico de cada elección, el entrenamiento sobre las lenguas habladas en la jurisdicción de interés, la identificación de las plataformas clave en que se difunde la información falsa y la incorporación de observadores humanos. Las alianzas con diversas plataformas, con organizaciones de comprobación de datos y con otros actores de interés podrían ser de utilidad para acceder, eliminar y responder a la información falsa sobre las elecciones.

Riesgos. Una dependencia excesiva de la IA para la detección de información falsa podría ocasionar que los organismos electorales pasaran por alto temas y preocupaciones clave, especialmente en plataformas de mensajería privada (por ejemplo, WhatsApp) donde la disponibilidad de datos es limitada. La mayoría de los LLM han sido optimizados principalmente en idioma inglés, y a menudo para ser usados en el contexto estadounidense, lo que podría motivar que los modelos pasaran por alto detalles importantes. La adecuada detección de información falsa requiere una comprensión clara de lo que constituye información falsa y de la legalidad de la actuación policial o de la respuesta a esta. Los organismos electorales pueden mitigar estas preocupaciones si utilizan la IA solo como un componente de una estrategia más amplia para identificar información falsa. Podrían surgir cuestiones relacionadas con la libertad de expresión, la vigilancia y el monitoreo gubernamental de las plataformas públicas, en especial por su vínculo con los derechos humanos y la libertad de expresión (CIDH, 2017).

Seguimiento de campañas y medios de comunicación

Caso de uso de la IA. En muchas jurisdicciones los organismos electorales son responsables de supervisar el contenido y la programación de las comunicaciones de las campañas, de otros grupos políticos y de los medios de comunicación. Por ejemplo, en algunos países existe un período de veda electoral previa a la votación y la IA puede contribuir a detectar infracciones de esa prohibición de las actividades de campaña. Los LLM adecuadamente ajustados con los flujos de datos de las redes sociales y de Internet pueden ser útiles para alertar sobre la existencia de contenido específico que incumpla las directrices del organismo electoral. Se trata de un proceso similar al proceso descrito para detectar la información falsa.

Implementación. En comparación con las acciones dirigidas a la detección de información falsa, en este caso será preciso implementar la tarea de seguimiento en función de las necesidades que se vayan identificando, ya que hasta el momento no se ha trabajado mucho en esta cuestión. Los LLM pueden ser ajustados en función de conjuntos de datos de contenido “permitido” y “no permitido”, y luego pueden ser abastecidos con información proveniente de las cuentas en redes sociales pertenecientes a las campañas políticas y las organizaciones de medios de comunicación para alertarlas sobre posibles infracciones.

Riesgos. Como en el caso de la detección de información falsa, una preocupación importante se relaciona con la excesiva dependencia respecto de las herramientas basadas en la IA para cumplir esta tarea, ya que es probable que dichas herramientas pasen por alto posibles infracciones. Además los modelos podrían actuar de manera discriminatoria, ya que, por ejemplo, podrían identificar más infracciones de un determinado partido político debido al diseño deficiente de los datos de entrenamiento. Esto podría tener consecuencias discriminatorias si la labor de seguimiento basada en la IA no se equilibra con otras formas de observación. Para abordar algunas de estas preocupaciones, los organismos electorales que están considerando implementar este caso de uso deben analizar la posibilidad de utilizar la IA como una pieza de una estrategia más amplia de seguimiento de los medios de comunicación y de las campañas electorales.

2.3.2. **Operaciones de votación**

Documentos de identificación de los votantes

Caso de uso de la IA. Los modelos de IA pueden ser útiles para verificar los documentos de identificación de los votantes. Muchos gobiernos y organismos electorales ya están utilizando herramientas tecnológicas para escanear documentos de identificación y compararlos con las bases de datos existentes, y la IA puede mejorar el grado de exactitud de estas tecnologías. Los modelos, por ejemplo, pueden permitir a los funcionarios electorales confirmar que la dirección de un votante se encuentra dentro de los límites del distrito electoral.

Implementación. Dado que muchos organismos electorales ya utilizan herramientas de *hardware* y de *software* para la verificación de los documentos de identidad, la aplicación de la IA puede implicar la actualización de los modelos que se usan para escanear y verificar documentos. Es probable que los modelos supervisados, entrenados a partir de documentos de identificación legítimos e ilegítimos, sean los más útiles para realizar esta tarea. Las herramientas de reconocimiento óptico de caracteres (OCR) y de reconocimiento óptico de marcas (OMR) basadas en la IA pueden ser útiles para escanear e indagar sobre formas de identificación no convencionales.

Riesgos. En muchos casos las herramientas de comprobación de la identidad se basan en el escaneado de códigos de barras, bandas magnéticas o chips de seguridad incluidos en los documentos y los

carnets de identidad. Es probable que estas herramientas tengan un mejor desempeño que los modelos de IA, ya que no se basan en inferencias o predicciones, y es posible que los modelos de IA sean menos exactos que las formas tradicionales de comprobación de la identidad. También cabe señalar que en países con bajas tasas de fraude electoral o con bajas tasas de tenencia de documentos de identidad es probable que requerir la identificación de los votantes prive a muchos de ellos de su derecho al voto sin incrementar la seguridad de las elecciones (Hajnal, Kuk y Lajevardi, 2018).

Biometría y comprobación de la identidad de los votantes

Caso de uso de la IA. Como se ha señalado en la subsección sobre registro y elegibilidad de votantes, los modelos de IA pueden ser útiles para los países que utilizan el reconocimiento biométrico (basado en los ojos, el rostro, la palma de la mano o las huellas dactilares) para la comprobación de la identidad de los votantes. Un modelo puede comparar los datos biométricos presentados por una persona durante el registro o en otros procesos oficiales con los datos biométricos de la persona que entrega la boleta electoral. Esto podría facilitar la autentificación de los votantes que carecen de documentos de identificación y podría mejorar la seguridad de las elecciones.

Los modelos de IA pueden ser útiles para los países que utilizan el reconocimiento biométrico para comprobar la identidad de los votantes.

Implementación. La implementación de esta tarea supone un proceso de dos pasos: el primero consiste en diseñar un sistema para capturar información biométrica durante el proceso de registro (ver la subsección sobre registro y elegibilidad de votantes) y el segundo consiste en verificar esos datos biométricos en el recinto electoral. Es en esta parte del proceso cuando es más probable que se utilice la IA, y en particular los modelos de aprendizaje profundo que permiten comparar *hashes* biométricos. Es probable que estos modelos sean desarrollados por proveedores externos, ya que requieren grandes conjuntos de datos de entrenamiento, y es poco probable que los organismos electorales tengan la capacidad de construirlos ellos mismos. Como se ha mencionado anteriormente, en 2016 el 35 por ciento de los organismos electorales encuestados capturaban datos biométricos durante el proceso de registro (Wolf et al., 2017). Algunos países, incluida India, están implementando programas piloto de uso de esos datos para la identificación de los votantes (Livemint, 2022). Las herramientas de comparación de firmas basadas en la IA también se utilizan regularmente en las elecciones, y al menos 29 de los condados más grandes de Estados Unidos las emplean para verificar los votos por correo (Bender, 2022).

Riesgos. Como ya se ha mencionado en la subsección sobre registro y elegibilidad de votantes, el fraude electoral es extremadamente raro en muchas jurisdicciones y los métodos de comprobación podrían causar más perjuicios que beneficios, dependiendo de las circunstancias específicas de cada país (Deepak, Simoes y MacCarthaigh, 2023). Además, la exactitud de las herramientas de comparación de firmas podría ser tan solo del 74,3 por ciento y su uso, por tanto, podría privar del derecho al voto a votantes elegibles (Hussain et al., 2015). También cabe señalar que, aunque las tasas de error de los sistemas biométricos a menudo son bajas, cuando estos sistemas fallan pueden afectar en mayor medida a las personas afrodescendientes, lo que constituiría una privación de derechos discriminatoria (Deepak, Simoes y MacCarthaigh, 2023; Wolf et al., 2017). Así, los sistemas biométricos conllevan graves riesgos que podrían afectar la seguridad de los datos, la privacidad y la realización de los derechos humanos, y podrían disuadir a muchas personas de participar en los procesos electorales. Esto plantea cuestiones relativas a la proporcionalidad: ¿los posibles riesgos en términos de seguridad, las preocupaciones relativas a los derechos humanos y la probabilidad de privar de sus derechos a ciertos grupos son más importantes que las ventajas de la identificación biométrica?

2.3.3. **Monitoreo de los centros de votación**

Detección de incidentes en los recintos electorales

Caso de uso de la IA. En los últimos años los votantes a menudo han publicado quejas en las redes sociales debido a problemas experimentados durante las elecciones y en los centros de votación. Las quejas hacen referencia a máquinas que no funcionan y largas colas, denuncian la supresión de votantes o describen comportamientos ilegales. Es posible utilizar los LLM para hacer un seguimiento de las plataformas de las redes sociales e identificar estos reportes, clasificarlos automáticamente y remitirlos a las autoridades competentes.

Implementación. Existen pruebas de que los LLM adecuadamente ajustados han podido detectar reportes de incidentes en los centros de votación durante las elecciones estadounidenses con un alto grado de exactitud (Juneja y Floridi, 2023). Su implementación requiere tener acceso a los datos de las redes sociales, lo que probablemente podría realizarse por medio de colaboraciones con diversas plataformas, para seleccionar palabras clave específicas relacionadas con las elecciones y crear conjuntos de datos

identificados bajo las etiquetas “incidentes” y “no incidentes”. Como en el caso de la detección de información falsa, es preciso que observadores humanos verifiquen los posibles incidentes para garantizar su seguimiento.

Riesgos. Aquí surgen preocupaciones similares a las relativas a la identificación de información falsa en las plataformas de las redes sociales, y también se debe considerar la posibilidad de omitir información valiosa debido a la dependencia excesiva de las soluciones de IA y al desempeño desigual de la tecnología y las personas. Esto significa que las herramientas deben utilizarse como complementos de los métodos existentes para la detección de incidentes en los centros de votación. Por otra parte, la recopilación masiva de datos públicos por parte de los gobiernos, especialmente en lo que respecta a temas políticos, plantea serias preocupaciones en torno a la vigilancia, la privacidad y los derechos humanos, y podría representar un desafío para la realización de la libertad de expresión (CIDH, 2017).

Videovigilancia

Caso de uso de la IA. La videovigilancia basada en la IA puede cumplir varias funciones durante las elecciones. Los modelos de IA que utilizan circuitos cerrados de televisión para vigilar los centros de votación podrían detectar incidentes o anomalías (por ejemplo, si un conjunto de imágenes registradas por los circuitos cerrados de televisión tiene un aspecto diferente en comparación con el conjunto medio de imágenes). Los modelos de IA también podrían ser útiles para detectar el fraude electoral si una persona aparece dos veces en el mismo centro de votación o si se registra su presencia en varios centros de votación diferentes (Deepak, Simoes y MacCarthaigh, 2023). En todos los casos se podrían señalar estos incidentes para que los funcionarios del organismo electoral o los observadores electorales realicen el seguimiento.

Implementación. La implementación requerirá contar con amplias capacidades en términos de circuitos cerrados de televisión y con la infraestructura necesaria para cargar las imágenes de las cámaras en los modelos de reconocimiento de imágenes y de videos basados en la IA. También puede ser importante ajustar los modelos para que puedan realizar tareas como el reconocimiento facial y la detección de anomalías (por ejemplo, se podrían etiquetar los comportamientos adecuados e inadecuados que se registran en los centros de votación).

Riesgos. Se sabe que las herramientas de videovigilancia basadas en la IA actúan de forma discriminatoria, y hay pruebas de que la tecnología de reconocimiento facial comete muchos más errores al identificar rostros no blancos, mientras que la probabilidad de error disminuye al identificar rostros blancos (Perkowitz, 2021). La inexactitud de los modelos, más que nada en lo que se refiere a la detección de casos de fraude, puede dar lugar a preocupaciones respecto de la integridad electoral y podría aumentar la carga de trabajo de los organismos electorales y de los equipos encargados de investigar el fraude electoral. Además, cualquier forma de vigilancia masiva, especialmente si es implementada por gobiernos, puede conllevar graves riesgos en lo que respecta al cumplimiento de los derechos humanos. Es probable que este aspecto disuada de participar a los votantes preocupados por su privacidad o a las personas que históricamente han sido objeto de ataques por ejercer su libertad de expresión y su derecho al voto.

2.3.4. **Tabulación y análisis de los votos**

Recuento y tabulación

Caso de uso de la IA. Los sistemas de OCR y OMR, que utilizan herramientas tecnológicas para leer formularios que han sido completados y escritos, ya se usan regularmente para el recuento y la tabulación de boletas electorales, ya sea impresas o enviadas por correo. Estos sistemas reconocen diferentes diseños de boletas, incluidas las boletas creadas específicamente para sistemas de OCR y OMR o las diseñadas para ser completadas manualmente. Además es posible utilizar estos sistemas en diferentes etapas del proceso: cuando los votantes entregan sus boletas, en los centros de votación, para leer los votos que llegan por correo postal, cuando el conteo se centraliza y para leer las actas de resultados. Los sistemas de OCR y OMR también se pueden utilizar para escanear firmas. La IA puede mejorar los sistemas tradicionales de OCR y OMR, ya que los casos más difíciles suelen servir como problemas para los sistemas automatizados existentes (Zhao et al., 2023). Esos sistemas podrían utilizarse para detectar diferencias o anomalías paralelamente al uso de los métodos habitualmente utilizados para el recuento de votos. Dichos sistemas pueden incluir, por ejemplo, modelos de IA de reconocimiento de imágenes entrenados para contar boletas de papel, reconocer texto escrito a mano para votar por candidatos no registrados en las boletas, o reconocer y verificar firmas.

Implementación. Las herramientas de comparación de firmas basadas en la IA desarrolladas por empresas privadas se utilizan

ampliamente en las elecciones para verificar los votos que se emiten por correo, y herramientas similares pueden utilizarse para el recuento de votos que requieran firmas (Bender, 2022). En muchos países las herramientas existentes aprovechan formas rudimentarias de la IA para contar boletas de papel estandarizadas y escaneables (MIT Election Lab, 2023). Según los resultados de algunas investigaciones los enfoques basados en el aprendizaje profundo han permitido lograr mejoras con respecto a la tecnología tradicional, con una exactitud probada de hasta el 99,984 por ciento (Barretto et al., 2021; Zhao et al., 2023).

Riesgos. Si bien hay pruebas de que los sistemas basados en la IA tienen un mejor desempeño que las tecnologías tradicionales de recuento automatizado de boletas, incluso índices de error muy bajos son motivo de preocupación pues podrían comprometer la integridad electoral y la confianza pública en las elecciones. Esto es especialmente cierto en lo que respecta al uso de modelos de aprendizaje profundo no interpretables, pues podría resultar difícil explicar al público los errores y los casos más difíciles. Además, la exactitud de las herramientas de comparación de firmas podría ser tan solo del 74,3 por ciento (Hussain et al., 2015). En Indonesia, por ejemplo, un sistema basado en OMR y OCR para escanear las hojas de resultados, Sirekap, ha generado controversia pues se han reportado irregularidades en los datos usados para el recuento de votos (Suhenda, 2024). Para mitigar estos riesgos los organismos electorales deben realizar pruebas comparativas con métodos disponibles, implementar la supervisión humana y considerar el uso de la IA como un método adicional, y no de reemplazo, para el recuento de votos.

Análisis de la participación y detección de anomalías en tiempo real

Caso de uso de la IA. Muchos organismos electorales examinan regularmente los índices de participación durante la jornada electoral con el fin de gestionar la logística y detectar posibles anomalías, y en ocasiones publican esos índices. La IA, tanto bajo la forma de modelos estadísticos tradicionales como bajo la forma de modelos de aprendizaje profundo (*machine learning*), puede ser útil para aumentar el valor de esos datos mediante el seguimiento de las métricas de participación en los centros de votación o en zonas geográficas específicas donde la realidad difiere significativamente de las expectativas. Ese seguimiento podría servir para alertar sobre posibles problemas, como el desarrollo de incidentes en los

centros de votación, la supresión de votantes o los intentos de fraude electoral, que los funcionarios podrían decidir investigar.

Implementación. A pesar de que no fue posible encontrar ningún estudio sobre el análisis en tiempo real de una elección, su implementación deberá ser similar a la de las auditorías poselectorales. Los modelos desarrollados antes de una elección con predicciones sobre la participación de votantes y sobre los resultados pueden compararse durante la jornada electoral con los resultados directamente procedentes de los centros de votación. En caso de identificarse diferencias significativas entre los resultados previstos y los reales, los organismos electorales podrían optar por investigar determinados centros de votación para establecer si hay algún problema.

Riesgos. En vista de que es poco probable que las simulaciones preelectorales produzcan resultados perfectamente exactos, los modelos desarrollados para detectar anomalías en la participación durante la jornada electoral pueden tener una alta probabilidad de producir falsos positivos. Esto podría dar lugar a una inadecuada asignación de los recursos del organismo electoral para investigar los centros de votación, lo que podría generar interferencias en centros de votación perfectamente funcionales y ocasionar que se omitan problemas reales en otros centros. El desarrollo de sistemas seguros y exactos para este caso de uso constituye una tarea técnicamente difícil, puesto que los modelos no solo deben asumir la tarea de por sí difícil de predecir los índices totales de participación, sino que además deben explicar cómo puede variar la participación a lo largo del período electoral.

Recuadro 2.1. **Elecciones digitales**

Cabe señalar que la IA puede ser útil para los países que están explorando nuevas formas de votación y elecciones. Por ejemplo, en países que cuentan con sistemas de votación en línea en que los votantes utilizan sus propios dispositivos, la IA puede contribuir al desarrollo de varias tareas. Los sistemas de votación en línea, por ejemplo, pueden utilizar un *software* de reconocimiento facial basado en la IA para identificar a los votantes, pueden usar modelos creados para detectar la actividad de bots o datos anómalos en páginas web para examinar posibles casos de fraude electoral, y pueden utilizar modelos entrenados para buscar amenazas de ciberseguridad y proteger la integridad de los servidores. La IA también puede ser útil para crear usuarios simulados que permiten probar los sistemas de votación en línea e identificar vulnerabilidades y posibles problemas.

En los países que están explorando nuevas formas de gobernanza democrática, como la democracia participativa en línea, los LLM pueden ayudar a resumir las posiciones y creencias de los votantes y los modelos de agrupamiento pueden contribuir a reunir ideas y declaraciones similares (Eisen et al., 2023). Por ejemplo, los países que deseen recibir comentarios sobre políticas específicas podrían crear plataformas para que los usuarios compartan comentarios y opiniones y luego podrían utilizar una combinación de IA y supervisión humana para comprender mejor las creencias de los participantes y en algunos casos lograr, incluso, soluciones de compromiso. En Taiwán el programa vTaiwan utiliza la plataforma Polis para recabar comentarios participativos sobre posturas políticas. Se utilizan modelos de IA para resumir y agrupar los comentarios y *chatbots* que hablan en nombre de posturas específicas (Landemore, 2023).

2.4. **FASE POSELECTORAL**

La fase poselectoral es la parte del ciclo electoral en que la mayor parte de la atención se centra en la revisión, el análisis, la modificación y la formulación de estrategias para la próxima elección.

2.4.1. **Análisis de los resultados electorales y elaboración de informes**

Auditorías poselectorales

Caso de uso de la IA. La IA puede ser útil para las actividades de auditoría poselectoral. Por ejemplo, se puede utilizar la IA para detectar casos de fraude, mientras que los modelos desarrollados antes de la elección permiten hacer comparaciones con los resultados reales. También es posible utilizar el aprendizaje automático y las estadísticas tradicionales, como el estimador de

diferencias en diferencias, para evaluar la eficiencia y la asignación de recursos de varios centros de votación. Los algoritmos de agrupamiento pueden ser útiles para detectar los centros de votación que presentan diferencias significativas con respecto a otros centros electorales.

Implementación. En diversas investigaciones se ha examinado el papel que pueden desempeñar los algoritmos entrenados a partir de datos electorales, tanto los no supervisados como los supervisados, en la detección del fraude electoral. En algunos casos esos modelos aplican técnicas de simulación entrenadas a partir de encuestas y otros datos electorales para determinar el grado de similitud entre los resultados reales y los simulados. Por lo general esos modelos requieren niveles elevados de fraude para proporcionar un alto grado de exactitud, de precisión (es decir, un bajo número de falsos positivos) y de sensibilidad (es decir, un bajo número de falsos negativos) (Yamin et al., 2023). En lugar de encuestas, en otros casos se han utilizado datos sintéticos con los que se generó una versión manipulada y otra no manipulada de los resultados electorales para entrenar un modelo que luego es aplicado a otras elecciones. En este trabajo se ha encontrado evidencia que señala que esta técnica podría constituir un punto de partida útil para futuros análisis forenses de las elecciones (Zhang, Álvarez y Levin, 2019). Los algoritmos no supervisados también pueden ser útiles en este caso, pues permiten a los organismos electorales agrupar los centros de votación y buscar y alertar sobre posibles anomalías (Green, 2021). Los organismos electorales deben considerar el uso de umbrales de probabilidad predefinidos para descartar los falsos positivos (por ejemplo, podrían examinar únicamente zonas geográficas en que los modelos han predicho una probabilidad de fraude superior al 90 por ciento).

Riesgos. Dado que es poco probable que los organismos electorales tengan acceso a conjuntos de datos en que los casos de fraude electoral estén perfectamente etiquetados, es difícil desarrollar modelos supervisados adecuados para realizar las auditorías poselectorales. La falta de datos reales hace que sea difícil evaluar la idoneidad de cualquier modelo. Una sensibilidad baja y una dependencia excesiva pueden ocasionar que los organismos electorales no detecten los casos de fraude electoral y otros problemas, mientras que una precisión baja puede dar lugar a que los organismos electorales investiguen una gran cantidad de falsos positivos. Ambos problemas podrían socavar la confianza de la ciudadanía en la integridad electoral. Los organismos electorales que están evaluando la posibilidad de implementar este caso de uso de la IA podrían mitigar algunos de estos riesgos considerando a este uso como una pieza más en el marco de un enfoque de auditoría más amplio.

Consolidación del financiamiento político

Caso de uso de la IA. La IA puede desempeñar un papel valioso en la consolidación y la auditoría de documentos e informes sobre el financiamiento político durante y después de una elección. Los modelos de OCR permiten escanear recibos físicos y los modelos de comparación permiten desarrollar pistas de auditoría a partir de informes sobre el financiamiento político. También pueden ser útiles los LLM y los modelos de integración para consolidar varios gastos y donaciones de campaña en formatos estandarizados que puedan ser revisados por los funcionarios electorales. Además, la IA puede ser útil para detectar casos de fraude en el financiamiento político, como los casos en que hay personas que hacen donaciones con nombres o direcciones diferentes o que hacen donaciones que no pueden ser aceptadas.

Implementación. Si bien no fue posible encontrar investigaciones en que se analice este caso de uso específico, la IA se utiliza cada vez más en las auditorías financieras de empresas, por lo que cabe considerar algunas prácticas de ese sector, posiblemente transferibles. Por ejemplo, las cuatro empresas de contabilidad más grandes del mundo (Deloitte, EY, KPMG y PwC) ofrecen un tipo de herramientas de IA para auditorías corporativas, que incluyen elementos como la detección de anomalías, la detección de fraude, las auditorías automatizadas de efectivo y la detección de patrones (Üçoğlu, 2020). Podría ser útil realizar algunas modificaciones a herramientas similares para rastrear las donaciones y los gastos políticos. Se pueden utilizar herramientas de reconocimiento de imágenes y de OCR para incorporar datos de entrada, y las herramientas de la IAG podrían ser útiles para organizar la documentación de los informes en formatos de datos estandarizados que serán usados para alimentar los sistemas de auditoría.

Riesgos. Las herramientas de la IA que se utilizan para consolidar datos pueden verse afectadas por alucinaciones u otros problemas de exactitud, lo que podría dar lugar a falsos positivos u ocasionar que los organismos electorales pasaran por alto información importante. Dado que aparentemente no se han creado herramientas específicas para la tarea de consolidar el financiamiento político, será preciso trabajar en el ajuste de las herramientas existentes para que puedan responder a las demandas particulares de los organismos electorales —tales como la incorporación de normativas sobre límites de las donaciones y los gastos—, que podrían incrementar la complejidad y disminuir la eficacia de los enfoques de IA.

Recuadro 2.2. **Uso de *chatbots* generalistas de IA en los organismos electorales**

Después de haber analizado casos de uso específicos de la IA para los organismos electorales, cabe hacer referencia a la manera más inmediata en que los organismos electorales pueden empezar a utilizar herramientas de la IA en su trabajo cotidiano: como apoyo para realizar todo tipo de tareas. Los *chatbots* basados en IAG, como ChatGPT de OpenAI, Copilot de Microsoft y Gemini de Google, ya se utilizan ampliamente en entornos personales y empresariales, y es probable que muchos funcionarios de organismos electorales ya hayan empezado a examinar oficialmente, o extraoficialmente, la capacidad de estas herramientas para mejorar la productividad interna.

En la mayoría de los casos se accede a estas herramientas principalmente a través de una interfaz de *chatbot*, en que los usuarios envían preguntas o comandos al modelo, que genera respuestas y otros datos de salida. Estas herramientas pueden usarse para resumir información de documentos existentes; redactar contenido para correos electrónicos, documentos o presentaciones, o consolidar información disponible en Internet. En algunos casos, por ejemplo con la integración de Copilot por Microsoft, los modelos pueden producir contenido que no sea texto, es decir que pueden generar imágenes, modificar hojas de cálculo o editar presentaciones.

Para los organismos electorales estas herramientas pueden constituir medios valiosos para apoyar la labor del personal, que puede recibir ayuda para redactar y resumir correos electrónicos, documentos y otros contenidos. Para el personal técnico, estas herramientas pueden constituir un apoyo útil para escribir, completar o comprobar códigos. Aunque hasta ahora el tema ha sido poco investigado, hay pruebas preliminares de que estas herramientas ofrecen un aumento modesto de la productividad laboral en entornos empresariales (Brynjolfsson, Li y Raymond, 2023; Noy y Zhang, 2023).

Cabe señalar que muchos gobiernos y empresas se encuentran todavía en las fases iniciales de prueba de estas herramientas y se necesita más información antes de poder elaborar recomendaciones específicas que establezcan si los empleados deberían utilizarlas, o cómo y cuándo deberían hacerlo. Los organismos electorales que están evaluando la posibilidad de utilizar estas herramientas deberían trabajar con otras entidades gubernamentales y en estrecha colaboración con los proveedores para crear programas piloto controlados y supervisados y así determinar en qué contexto podrían ser útiles (Carrasco et al., 2024).

Como ocurre con otros casos de uso de la IA, la utilización de estas herramientas de la IA genera preocupaciones, sobre todo respecto de la confiabilidad y seguridad. La principal preocupación que suscita el uso de estas herramientas en los organismos electorales se relaciona con su propensión a alucinar. Esto puede constituir un problema grave, especialmente cuando la información se utiliza para redactar material de divulgación pública (Rawte, Sheth y Das, 2023). Otra preocupación surge cuando estas herramientas se utilizan para resumir información proveniente, por ejemplo, de

Recuadro 2.2. **Uso de *chatbots* generalistas de IA en los organismos electorales (cont.)**

documentos legales, pues podría ocurrir que las herramientas no incluyan información importante, que alucinen o que tergiversen información del documento original. En términos generales no se puede confiar plenamente en los datos de salida de estas herramientas, lo que complica la posibilidad de utilizarlas para diversos fines.

Además, si bien muchas de estas herramientas cuentan con versiones empresariales que se basan en protocolos de seguridad mejorados, las necesidades y responsabilidades de seguridad de los gobiernos suelen ser más estrictas, especialmente cuando se trata de información sensible. Dependiendo de la herramienta utilizada, existe el riesgo de que los datos introducidos por los usuarios se incorporen a los datos de entrenamiento de la herramienta, lo que podría dar lugar a la filtración de información interna. Algunas entidades gubernamentales han prohibido el uso de estas herramientas a nivel interno, debido a reparos sobre su seguridad (Solender y Fried, 2024).

A pesar de que los riesgos enumerados son importantes, los organismos electorales podrían mitigar algunos de ellos. Por motivos de seguridad, muchas empresas de IAG están creando versiones de sus herramientas aptas para la administración pública que cumplen con normas más estrictas exigidas para su uso en el sector público (Solender y Fried, 2024). En vista de la novedad y el impacto potencial de esta tecnología los organismos electorales deberían considerar la realización de pruebas más exhaustivas que las habituales para comprobar la seguridad de las nuevas herramientas de *software*.

Puede resultar más difícil mitigar los riesgos relativos a la confiabilidad, especialmente en las fases tempranas de desarrollo de estas tecnologías. Estas herramientas podrían ser consideradas para casos de uso específicos; por ejemplo, el uso de la IA para resumir documentos de política que los organismos electorales utilizarán para la toma de decisiones constituye un caso de uso mucho más riesgoso que la utilización de estas herramientas para elaborar breves correos electrónicos internos. Los organismos electorales que están probando estas herramientas deberían hacer énfasis en los problemas de confiabilidad y deberían capacitar al personal de forma exhaustiva sobre la importancia de comprobar los hechos, garantizar las acciones de supervisión humana y realizar evaluaciones del riesgo que supone el uso de estas herramientas en determinados momentos y contextos.

2.5. **RETOS, RIESGOS Y ESTRATEGIAS DE MITIGACIÓN ADICIONALES**

El uso de la IA para la gestión electoral es prometedor en muchos ámbitos para mejorar los resultados, aumentar la eficiencia y crear sistemas más equitativos. Al mismo tiempo, a menudo introduce o exacerba una serie de riesgos graves.

En las secciones anteriores se presentaron una serie de preocupaciones y riesgos asociados al uso potencial de la IA por parte de los organismos electorales para desarrollar tareas específicas. Cabe destacar que en todos los casos existen importantes preocupaciones éticas, prácticas y relativas a los derechos humanos, que abarcan desde dificultades técnicas para su implementación hasta cuestiones serias relativas a la integridad electoral. Al margen de esas preocupaciones específicas, en esta sección el análisis se centra en cuestiones adicionales relacionadas con el uso de la IA como parte de la gestión electoral, a saber: las vulnerabilidades en materia de ciberseguridad, la consolidación privada de la infraestructura pública, los derechos humanos, los sesgos y la discriminación, y la confianza del público en las elecciones.

En algunos casos se trata de riesgos que es posible abordar; en otros casos, es probable que los riesgos surjan como resultado de cualquier uso que se haga de la IA. Si bien en cierta medida exceden el alcance de este informe, se examinan algunas posibles estrategias de mitigación para abordar algunas de estas preocupaciones y riesgos, y para promover que los organismos electorales emprendan la implementación de la IA mediante un proceso informado de análisis de las potencialidades y limitaciones de cada caso de uso.

En concreto cabe destacar tres conceptos del Reglamento General de Protección de Datos de la Unión Europea: la necesidad (es preciso establecer cuán importante es un caso de uso), la minimización de datos (es preciso recopilar solo la cantidad de datos mínima necesaria para un caso de uso) y la proporcionalidad (es preciso asegurarse de que las desventajas que supone perder privacidad no pesen más que las ventajas de limitar la privacidad).

Cabe señalar que en muchos casos puede ser útil centrarse en procesos de supervisión humana exhaustivos de los sistemas de IA para atenuar muchos de los riesgos detallados en este informe. Por ejemplo, el riesgo potencial de utilizar la IA para decidir

dónde asignar al personal electoral aumenta significativamente si esas recomendaciones se implementan sin que el personal del organismo electoral experto en la materia realice pruebas y controles exhaustivos. Dado que la trayectoria de muchos de estos posibles casos de uso no se ha probado ni se investigado suficientemente, es muy importante contar con procesos exhaustivos de supervisión humana en las fases piloto. Una posible estrategia de mitigación consiste en ejecutar en paralelo versiones automatizadas y versiones dirigidas por personas de cada caso de uso, y comparar los resultados.

2.5.1. **Preocupaciones generales y estrategias de mitigación**

Marco jurídico

El uso de la IA en las elecciones requiere contar con una comprensión profunda de los marcos jurídicos y regulatorios a fin de establecer si es posible —y cuándo es factible— utilizar tecnologías digitales e implementar la toma de decisiones automatizada en los procesos electorales. Es posible que los usos de la IA en los procesos electorales requieran una actualización de las leyes electorales vigentes, así como una actualización de las normas que regulan el uso de la tecnología por parte de autoridades públicas y contrataciones públicas. Además, varias jurisdicciones están introduciendo normativas sobre la IA que pueden establecer requisitos y restricciones adicionales para el uso de estas tecnologías en la administración de las elecciones y en los procesos democráticos, como es el caso del Reglamento de Inteligencia Artificial de la Unión Europea. Este tema se analiza más detenidamente en el capítulo 4.

Riesgos relativos a la ciberseguridad

Es probable que cualquier uso de la IA en el marco de las elecciones genere nuevas preocupaciones relativas a la ciberseguridad, además de las amenazas cibernéticas adicionales impulsadas por la IA y procedentes de otros actores (ver capítulo 3). En lo que respecta a la implementación, los riesgos en términos de ciberseguridad son dobles: en primer lugar, el uso de más tecnologías digitales aumenta el área de ataque (o los puntos de entrada) de los ciberatacantes, lo que significa que estos tendrán más oportunidades de identificar vulnerabilidades en un sistema electoral. La creciente dependencia de las tecnologías digitales como parte del proceso electoral brinda nuevas oportunidades a los atacantes para dañar la integridad de las elecciones. En segundo lugar, el uso de la IA como parte del proceso electoral también requiere que los organismos electorales recopilen

más tipos de datos, ya sea sobre los votantes o sobre la elección, entre los que se incluyen datos biométricos de los votantes o imágenes de las cámaras dispuestas en los centros de votación. Esto aumenta la cantidad de datos que son valiosos para los atacantes, y también acrecienta los daños que supondría un ciberataque exitoso. El uso de la IA por parte de actores malintencionados puede incrementar la sofisticación de los ciberataques. En la práctica, la preocupación por la ciberseguridad podría dañar la integridad de las elecciones tanto directa como indirectamente. Directamente, los ciberataques exitosos pueden impedir que la ciudadanía vote, modificar los resultados, alterar las bases de datos del registro de votantes y corromper los datos. Indirectamente, los ciberataques no exitosos, o incluso tan solo la amenaza de un ciberataque, podrían erosionar la confianza pública en el sistema electoral y disuadir a ciertos grupos de la población de participar en las elecciones.

En muchos casos se trata de preocupaciones y riesgos que es posible mitigar. Con el fin de atenuar los riesgos en materia de ciberseguridad asociados al uso de la IA, los organismos electorales deben considerar la colaboración con agencias y expertos en ciberseguridad para realizar auditorías de la ciberseguridad de los sistemas electorales y así salvaguardar estos nuevos puntos de entrada. Respetar el principio de minimización de datos también puede disminuir el riesgo general en términos de ciberseguridad, por lo que los organismos electorales deben poner el foco en recopilar la menor cantidad posible de datos privados y solo recabar los datos indispensables para realizar funciones específicas de la IA.

Dependencia excesiva respecto de las empresas privadas

Dadas las dificultades que plantea la implementación técnica de muchos de estos casos de uso, la creciente dependencia de los organismos electorales respecto de las empresas privadas es otro tema que causa preocupación. Como mínimo el uso de la IA requiere contar con infraestructura técnica como las unidades de procesamiento de gráficos, cuya producción y mantenimiento están en manos de un pequeño grupo de empresas. En muchos casos es probable que los organismos electorales necesiten infraestructura informática adicional (por ejemplo, computación en la nube), talento técnico de empresas privadas y asistencia para desarrollar las prácticas de ciberseguridad. El cumplimiento de estos requisitos puede implicar que un selecto grupo de empresas tenga cada vez más poder sobre la administración de las elecciones, lo que genera preocupación por la influencia del sector privado en los gobiernos y la política (Jungherr, 2023).

Además, las herramientas de la IA probablemente sean desarrolladas por proveedores tradicionales de tecnologías electorales. Cabe esperar que la incorporación de esas tecnologías sea compatible con las prácticas habituales de los organismos electorales, pero es importante señalar que su incorporación probablemente requiera que los organismos electorales realicen muchas más pruebas y análisis que antes.

Para empezar a mitigar algunos de estos riesgos, los organismos electorales deben trabajar con otras entidades gubernamentales para examinar qué casos de uso de la IA podrían desarrollarse internamente y cuáles requerirían alianzas con el sector privado. Los organismos electorales deben considerar la posibilidad de realizar auditorías más exhaustivas de las tecnologías desarrolladas por el sector privado y establecer estándares elevados para garantizar la eficacia y la equidad en el trato con los proveedores. También puede ser importante establecer normas sobre la transparencia y la rendición de cuentas de las tecnologías desarrolladas por el sector privado, en especial a la hora de considerar las políticas estatales sobre acceso a la información relativa a los procesos de toma de decisiones gubernamentales.

Sesgos, discriminación, vigilancia y derechos humanos

Existe un largo historial de uso de la IA y de las técnicas estadísticas tradicionales para discriminar a determinados grupos de personas, por ejemplo mediante el encarcelamiento masivo, la denegación de prestaciones o la discriminación electoral (Crawford, 2022). La ética de la IA es un tema ampliamente estudiado, por lo que en este informe se abordan brevemente los aspectos que requieren un análisis más detallado por parte de los organismos electorales. Cualquier uso de los sistemas de IA que implique la recopilación de grandes cantidades de datos, principalmente por parte de los gobiernos, conlleva el riesgo de perpetuar la vigilancia y las violaciones de los derechos humanos asociadas con esa vigilancia. Por ejemplo, la IA que se basa en la recopilación masiva de contenidos públicos en las redes sociales puede constituir una práctica de vigilancia que tenga el efecto de mermar la libertad de expresión, incluso aunque no se haga un uso indebido de esos datos (CIDH, 2017). La IA que se basa en datos biométricos genera preocupaciones similares, ya que puede disuadir a las personas de participar en los procesos electorales por reparos vinculados con la privacidad o la seguridad.

Estos riesgos se multiplican cuando se los examina a través de la lente de la discriminación, ya que la IA a menudo se utiliza para perpetuar los prejuicios existentes en la sociedad. Por ejemplo, es menos probable que los modelos de reconocimiento facial basados en la IA identifiquen correctamente a las personas afrodescendientes, la mayoría de los LLM son entrenados principalmente con datos en inglés y los algoritmos de la vigilancia policial predictiva tienden a perpetuar las fallas de los sistemas de justicia (Perkowitz, 2021; Gstrein, Bunnik y Zwitter, 2019; Stokel-Walker, 2024). Dado que los modelos de IA suelen ser entrenados con datos producidos por personas o suelen basarse en el comportamiento humano, los sesgos existentes a menudo se amplifican en sus resultados.

Incluso en ausencia de una intención maliciosa, la IA y la recopilación masiva de datos por parte de los organismos electorales plantean graves riesgos para los derechos humanos: la acción de recopilar datos puede dar lugar al uso de esos datos para impedir o desalentar el voto o para vulnerar el anonimato de las personas, y existe la posibilidad de que se produzcan filtraciones de datos o de que los datos accidentalmente se usen de forma indebida. El uso de la IA y la recopilación de datos pueden ocasionar un aumento general de la sensación de vigilancia, lo que puede provocar un efecto de desaliento (que también se conoce como efecto disuasorio). El efecto de desaliento es el efecto negativo que una acción estatal (por ejemplo, la vigilancia) tiene sobre las personas, y dicho efecto disuade anticipadamente a las personas de ejercer sus derechos (por ejemplo, el derecho al voto) por miedo a las consecuencias formales o informales (Pech, 2021). Si actores malintencionados logran acceder a los datos en cuestión, los riesgos se incrementan ya que los datos sobre el voto, los datos de voz y video y los datos biométricos (todos ellos posibles fuentes de datos para los organismos electorales) podrían utilizarse para dañar explícitamente a los votantes.

Para minimizar algunos de estos riesgos los organismos electorales deben prestar especial atención a los principios de necesidad, proporcionalidad y minimización de datos mencionados anteriormente, y deben realizar un análisis exhaustivo de las posibles externalidades negativas y una ponderación de las ventajas y desventajas de cada caso de uso de la IA. Como se señala en el capítulo 4, en muchos enfoques de regulación de la IA se adopta un marco basado en los riesgos, que se centra en la definición de directrices sólidas para hacer frente a situaciones de alto riesgo.

Los organismos electorales deben trabajar con otras entidades y con grupos de expertos para examinar cómo el uso de la IA de alto riesgo podría impactar en los derechos humanos, por ejemplo a través de la vigilancia masiva y la restricción de la libertad de expresión. Además, los organismos electorales deben centrarse específicamente en analizar el impacto que los casos de uso pueden tener en la población más vulnerable. Dichos organismos deben considerar la posibilidad de realizar auditorías continuas basadas en principios éticos para evaluar los casos de uso de la IA (Mökander y Floridi, 2021). A fin de evitar la perpetuación de daños anteriores sería preciso prestar especial atención a los sesgos existentes en los datos de entrenamiento.

Confianza pública en las elecciones

Por último, existe el riesgo de que disminuya la confianza de la ciudadanía en las elecciones. Los usos visibles de la IA en el sistema electoral pueden generar escepticismo entre los votantes respecto de la imparcialidad y la seguridad de las elecciones (Deepak, Simoes y MacCarthaigh, 2023). En el caso de los usos menos visibles de la IA, como la gestión de las listas de votantes, la ciudadanía podría enterarse de estas prácticas por fuentes no oficiales y esto podría tener un impacto negativo adicional en la confianza. El papel del sector privado como parte del proceso electoral puede afectar aún más la confianza. Estas preocupaciones pueden ser muy significativas para diferentes grupos de población, especialmente en países con una historia sostenida de discriminación contra determinados grupos. El uso de modelos de aprendizaje profundo a menudo no interpretables puede agravar este problema, sobre todo por sus implicaciones para la transparencia gubernamental. Si los modelos se utilizan para tomar decisiones sobre temas como la ubicación de los centros de votación o la elegibilidad de los votantes, la ciudadanía o la normativa (por ejemplo, el Reglamento General de Protección de Datos de la Unión Europea) podrían exigir un nivel de transparencia (por ejemplo, la explicación sobre cómo y por qué se tomó una decisión) que los modelos podrían no estar en condiciones de proporcionar.

Para mitigar algunos de estos riesgos los organismos electorales deben promover el establecimiento de normas estrictas de transparencia para el uso de la IA, que incluyan explicaciones detalladas de los casos de uso y del papel que desempeña la IA en los procesos de toma de decisiones (Deepak, Simoes y MacCarthaigh, 2023). Como se ha mencionado anteriormente, una supervisión humana exhaustiva y el desarrollo mécanismos

de apelación son medidas que pueden contribuir a mitigar las preocupaciones de la ciudadanía. Centrarse en modelos de IA fáciles de interpretar, en vez de poner la atención en enfoques basados en el aprendizaje profundo, permitirá a los organismos electorales ofrecer explicaciones más exhaustivas a la ciudadanía sobre cómo y por qué se tomaron las decisiones en las que intervino la IA.

2.6. **LOS CAMINOS A SEGUIR**

Si bien el objetivo de este informe no es sugerir vías o casos de uso específicos que los organismos electorales deban empezar a implementar, a continuación se brinda una serie de recomendaciones para los organismos electorales interesados en explorar el uso de la IA para la gestión electoral.

1. Los organismos electorales deben aplicar los principios de necesidad, minimización de datos y proporcionalidad a la hora de considerar la implementación de la IA para la gestión electoral, y deben centrar sus acciones en los casos de uso que ofrezcan los mayores beneficios y que al mismo tiempo permitan minimizar las externalidades negativas.

2. Los organismos electorales deben considerar los casos de uso de la IA en el contexto de las prácticas existentes, centrándose en los ámbitos en que la IA puede mejorar los resultados actuales, y realizar comparaciones exhaustivas de los riesgos y las potencialidades de la implementación de la IA.

3. En la medida de lo posible, los organismos electorales deben procurar la supervisión humana de los sistemas de IA y deben centrarse en formas de incluir la IA junto con otras estrategias, en lugar de sustituirlas.

4. Los organismos electorales deben realizar auditorías exhaustivas y continuas de la seguridad, el desempeño y la ética de los sistemas de IA.

5. Los organismos electorales deben establecer normas sólidas de transparencia, interpretabilidad y rendición de cuentas, tanto para los sistemas de IA desarrollados internamente como para los suministrados por proveedores externos.

6. Los organismos electorales deben trabajar en estrecha colaboración con otras entidades, grupos de derechos humanos y grupos de interés comunitario a la hora de analizar la posibilidad de implementar y diseñar sistemas de IA.

7. Los organismos electorales deben identificar claramente, mediante la incorporación de una marca de agua, todos los contenidos generados por sistemas de IA.

8. Los organismos electorales que estén considerando la posibilidad de utilizar la IA deben centrarse en primer lugar en desarrollar su infraestructura interna, sus conocimientos técnicos y sus prácticas éticas y de auditoría, incluso si están pensando en adquirir herramientas de proveedores externos, para medir y gestionar adecuadamente la implementación de la IA y evaluar los riesgos que puede conllevar su uso.

Capítulo 3

EL USO DE LA IA POR PARTE DE OTROS ACTORES POLÍTICOS Y SUS EFECTOS EN LOS ORGANISMOS ELECTORALES

A corto plazo es probable que los principales efectos de los avances de la IA en los organismos electorales provengan de su uso durante las elecciones por parte de otros actores.

El objetivo central de este informe es examinar posibles usos de la IA para la gestión electoral. Sin embargo, a corto plazo es probable que los principales efectos de los avances de la IA en los organismos electorales provengan de su uso durante las elecciones por parte de otros actores. Así, en este capítulo se examinan algunas de las maneras en que diversos actores externos, como los organizadores de campañas políticas, los productores de información falsa y los *hackers*, pueden utilizar la IA para influir en las elecciones y en las actividades de los organismos electorales. También se analizan las posibles estrategias de mitigación que podrían desplegar los organismos electorales y otros actores destacados.

3.1. IAG E INFORMACIÓN FALSA

Quizá el tema más debatido en la intersección de la IA y las elecciones sea el papel que la IAG puede desempeñar en la creación y la divulgación de información política falsa. Dado que se trata de un tema muy amplio, en este informe el análisis se centra exclusivamente en la información falsa relevante para la gestión electoral y no en la información falsa sobre puntos de vista o candidatos políticos. Cabe señalar que la divulgación de información falsa impulsada por la IAG sobre candidatos y posiciones políticas ya está ocurriendo, y es probable que incida en la labor de los organismos electorales y que en especial afecte algunas de sus funciones, como mantener la integridad de las elecciones, conservar la confianza del público y prevenir la violencia electoral (Hsu, Thompson y Myers, 2024). En este informe el foco se centra en la información falsa sobre aspectos de los procesos electorales tales

como la fecha y el lugar de las elecciones, y también en las noticias falsas que comprometen la seguridad y la imparcialidad de las elecciones.

La información falsa como un medio de deslegitimación ya existía mucho antes de la llegada de la IA y sus avances. En investigaciones anteriores realizadas por el Instituto Internacional para la Democracia y la Asistencia Electoral (IDEA Internacional) se estudió el entorno informativo de 53 países y se descubrió que los tipos de desinformación más comunes eran los ataques a la imparcialidad de los organismos electorales, la información falsa o engañosa sobre los métodos y las condiciones de votación, y otros recursos para engañar a la ciudadanía a fin de que no votara (Bicu, 2023). Diversas técnicas de desinformación en línea y fuera de línea se utilizan desde hace tiempo para engañar a la ciudadanía —y en especial a los grupos de población más vulnerables— sobre la elegibilidad y la logística de las elecciones (Vandewalker, 2020).

En esta sección la pregunta principal es la siguiente: ¿de qué manera la IA exacerba este problema? La IAG aumenta la oferta de las formas tradicionales de desinformación, como las noticias falsas y las publicaciones engañosas en las plataformas de las redes sociales, y mejora su calidad. Al utilizar plataformas de IAG y modelos de código abierto los actores malintencionados pueden actuar con rapidez para generar contenidos de texto, audio y video con objetivos específicos centrados en grupos particulares. La calidad de esos contenidos suele ser similar o superior a la calidad de las noticias falsas tradicionales escritas por personas, y la probabilidad de detectar de forma automatizada la falsedad del contenido es menor (Zhou et al., 2023). Si bien es poco probable que el uso de estas plataformas y modelos incremente los problemas de desinformación en aquellos espacios en que esto ya era un motivo de preocupación (como las publicaciones dirigidas a públicos numerosos en las plataformas de las redes sociales), esta mejora de las capacidades representa un problema para espacios anteriormente desatendidos, como pequeñas comunidades en redes sociales que tal vez fueron ignorados por los atacantes en el pasado debido a limitaciones de tiempo y recursos. La principal amenaza de la información falsa basada en la IA posiblemente resida en el nivel comunitario, donde es menos probable que los organismos electorales se percaten de su propagación y donde las noticias falsas difundidas por actores malintencionados pueden estar hiperfocalizadas en grupos o individuos específicos. Es posible difundir información falsa en diversas plataformas, como

AI utilizar plataformas de IAG y modelos de código abierto los actores malintencionados pueden actuar con rapidez para generar contenido de texto, audio y video con objetivos específicos centrados en grupos particulares.

las principales redes sociales, las listas de correo electrónico, los motores de búsqueda y los servicios de mensajería privada. En este último caso, será difícil detectar la información falsa, ya que las plataformas de mensajería encriptada no pueden moderar el contenido que se comparte en los mensajes.

La IAG ofrece nuevas capacidades para la desinformación, incluida la creación de ultrafalsos o *deepfakes* de audio y video de alta calidad. Los riesgos asociados a estas formas de desinformación pueden variar en los distintos países. En Canadá y Estados Unidos, por ejemplo, se estima que una de las principales amenazas de la desinformación basada en la IA es el desarrollo de *deepfakes* de audio para imitar a candidatos políticos, funcionarios electorales y líderes comunitarios locales, y la utilización de esas imitaciones para llamar a los votantes y engañarlos con relación a los procesos electorales (Bond, 2024). Ya hay evidencia de que esto ocurre en las elecciones estadounidenses (Hsu, 2024). Esta amenaza es más pronunciada cuando se ejecuta en comunidades pequeñas y focalizadas, pues es menos probable que los funcionarios tomen conocimiento de la desinformación antes de su propagación.

Es probable que los *deepfakes* de video, que podrían constituir una amenaza importante en otros países, se utilicen con fines similares. Si bien los *deepfakes* de video todavía no logran imitar a la perfección el realismo de un video auténtico, causan una gran preocupación entre las comunidades que cuentan con niveles más bajos de alfabetización digital. Justo antes de las últimas elecciones generales de Pakistán se difundieron múltiples videos ultrafalsos en plataformas de todo el país, por ejemplo, videos falsos de políticos que llamaban a boicotear la elección, lo que pudo haber afectado la integridad electoral (Mughal, 2024). A pesar de que actualmente no hay pruebas del impacto de los *deepfakes* de video o audio sobre la integridad electoral en un contexto global, los organismos electorales deberían estar preparados para hacer frente a un aumento de la cantidad, y a una mejora de la calidad, de este tipo de desinformación.

Existe un riesgo adicional, y es que la difusión de información falsa de mejor calidad socave aún más la confianza de la ciudadanía en cualquier tipo de información en línea. Esto podría impulsar a los candidatos y a otros actores relevantes a utilizar el "dividendo del mentiroso" y a afirmar que determinadas grabaciones o imágenes auténticas han sido generadas por la IA. Es probable que esto ocasione una disminución general de la confianza en la información,

lo que dificultará la labor de los organismos electorales que están encargados de difundir información exacta. Además existen pruebas que demuestran que generar una preocupación excesiva entre la ciudadanía por la propagación de información falsa tiene pocas probabilidades de disminuir la desconfianza ante la desinformación, y al mismo tiempo es probable que ello incremente la disposición de las personas a apoyar restricciones de la libertad de expresión (Jungherr y Rauchfleisch, 2024).

Cabe señalar que, dado que el uso de *chatbots* basados en IA se ha extendido entre la población, los votantes podrían hacer preguntas a *chatbots* como el ChatGPT o Gemini sobre las elecciones, para saber, por ejemplo, cuándo tendrá lugar la votación, dónde se puede votar o si las elecciones son seguras. Al igual que en el caso de los votantes que utilizan motores de búsqueda para tal fin, este uso de los *chatbots* plantea preocupaciones relativas a la exactitud de la información. Dado que no todos los *chatbots* basados en LLM tienen acceso a Internet y que a menudo son entrenados a partir de información obsoleta, a lo que se suma su tendencia a alucinar, es lógico suponer que estos *chatbots* podrían proporcionar información incorrecta sobre la elegibilidad de los votantes y la logística de las elecciones. Algunas plataformas de IAG han anunciado su intención de asociarse con fuentes fidedignas de información electoral a las que podrían dirigir las preguntas de los usuarios, pero la eficacia y el alcance de estos planes, especialmente fuera de Estados Unidos, aún se desconocen (OpenAI, 2024).

3.2. **ORGANIZACIONES POLÍTICAS**

En varios países las campañas políticas están utilizando desde hace algún tiempo la ciencia de datos y las técnicas de aprendizaje automático como parte de sus estrategias. Entre los ejemplos recientes más destacados cabe mencionar el uso de la ciencia de datos para recaudar fondos y organizar la campaña presidencial de Barack Obama que se desarrolló en Estados Unidos en 2012, el escándalo de Cambridge Analytica que tuvo lugar en 2016 en el Reino Unido y en Estados Unidos, y el creciente uso de la ciencia de datos en las elecciones de India (Dommett, 2019; Varna, 2019).

En varios países las campañas políticas están utilizando desde hace algún tiempo la ciencia de datos y las técnicas de aprendizaje automático como parte de sus estrategias.

Es probable que las organizaciones políticas utilicen la IA para una variedad de tareas, algunas de las cuales pueden ser importantes para los organismos electorales. Existen pruebas

de que la publicidad política altamente personalizada y dirigida a audiencias microsegmentadas puede ser más eficaz que la publicidad genérica que se difunde en las plataformas de las redes sociales (Simchon, Edwards y Lewandowsky, 2024). Las campañas y distintas organizaciones políticas pueden utilizar la IA para desarrollar anuncios específicos dirigidos a individuos o a pequeños grupos de la población para influir en su comportamiento electoral. En los países en que los organismos electorales son responsables de monitorear las comunicaciones que se difunden durante la campaña electoral, el uso de la IA para generar distintas versiones de un mismo anuncio de campaña podría ocasionar un incremento importante de la carga de trabajo de dichos organismos. Es posible que los organismos electorales tengan que repensar los procesos que realizan para monitorear e informar sobre la publicidad desplegada en el marco de las campañas. Debido a la posibilidad de que los modelos de IAG alucinen o produzcan información falsa, los riesgos asociados a la publicidad de campaña podrían incrementarse, sobre todo cuando las organizaciones utilizan sistemas totalmente automatizados. Además, las organizaciones políticas podrían utilizar la IAG a sabiendas para desarrollar y difundir desinformación. Para resolver estos problemas podría ser preciso que los organismos electorales emitan más normas y ejerzan una mayor supervisión, y en algunos casos podría ser necesario que establezcan alianzas con otras entidades gubernamentales o que modifiquen sus mandatos.

Otras estrategias de las campañas orientadas al público y basadas en la IA también pueden ser relevantes para los organismos electorales. Hay candidatos políticos de todo el mundo que ya han utilizado la IAG para crear *deepfakes* de sí mismos en que aparecen pronunciando discursos o hablando en idiomas extranjeros (Calma, 2023; Zhuang, 2024). Para los organismos electorales responsables de hacer un seguimiento de las comunicaciones en el marco de las campañas, este uso de la IA puede plantear cuestiones complejas relativas a la definición de información falsa o de comunicación engañosa. En las campañas de varios países, como Indonesia y Pakistán, ya se ha empezado a crear *chatbots* finamente ajustados que imitan a los candidatos o que proporcionan información con la cual los votantes pueden interactuar (Parkin y Bokhari, 2024; Rayda, 2024). Los problemas que plantean estos *chatbots* son similares a los que plantean los *chatbots* generales, en el sentido de que las respuestas a las preguntas que hacen los usuarios con relación a las elecciones pueden no ser exactas.

Es probable que las organizaciones políticas utilicen la IA para una variedad de otras tareas de campaña, como la elaboración de discursos y contenidos, la asignación de recursos, la organización de estrategias, la elaboración de análisis internos y los ejercicios de colaboración masiva (*crowdsourcing*) respecto de posiciones políticas. En algunas ocasiones estos usos de la IA pueden repercutir en el trabajo de los organismos electorales. Por ejemplo, es posible que las campañas utilicen la IA para crear mejores capacidades de análisis de datos, lo que contribuiría a decidir dónde centrar las acciones publicitarias, las visitas o los eventos. Para los organismos electorales cuyo mandato es proteger el derecho de los votantes a la privacidad de los datos el uso de la IA puede conllevar riesgos porque generalmente requiere la utilización de conjuntos de datos más grandes en comparación con los métodos estadísticos tradicionales. Además, si esos métodos tienen éxito, ello podría repercutir en los índices de participación y obligar a los organismos electorales a reconsiderar la forma en que los recursos se asignan y se distribuyen entre los diferentes centros de votación y las distintas zonas geográficas.

3.3. **AMENAZAS PARA LA SEGURIDAD DE LOS SISTEMAS ELECTORALES**

Los sistemas electorales y los organismos electorales son desde hace tiempo el blanco de ciberataques.

Los sistemas electorales y los organismos electorales son desde hace tiempo el blanco de ciberataques (Van der Staak y Wolf, 2019). Si bien existen muchas amenazas en términos de ciberseguridad para los organismos electorales y otras entidades responsables de las elecciones, en este informe el análisis se centra exclusivamente en aquellos ámbitos en que los avances de la IA podrían exacerbar el problema a corto plazo, es decir, a través de intentos de ciberestafas de mejor calidad. Aunque es probable que los avances de la IA mejoren la calidad de los programas maliciosos (*malware*) y de las técnicas de desarrollo de programas intrusos (*exploits*), a corto plazo el principal riesgo de la IA para la ciberseguridad en relación con los organismos electorales es la cada vez mejor calidad de las ciberestafas (Centro Nacional de Ciberseguridad, 2024).

Los piratas informáticos que atacan procesos electorales suelen utilizar la ingeniería social (es decir, tácticas para manipular, influir o engañar a las víctimas) para tener acceso a sistemas privados, por lo general mediante ciberestafas. Una ciberestafa (*phishing*) consiste en engañar a los destinatarios de un mensaje al hacerles

creer que las comunicaciones proceden de fuentes de confianza y aprovechar ese engaño para que las víctimas compartan información sensible o descarguen archivos dañinos. En el pasado los intentos de ciberestafa a gran escala generalmente eran de baja calidad, debido a que se necesita mucho tiempo para crear comunicaciones fraudulentas de alta calidad dirigidas a individuos específicos (es lo que se conoce comúnmente como ciberestafa personalizada). Tal como ocurre con relación a la desinformación, la IAG hace que el proceso para encontrar víctimas potenciales y generar contenido de alta calidad sea sustancialmente más eficiente y, por tanto, incrementa las probabilidades de éxito (Norden y Ramachandran, 2023). El ajuste de los modelos de lenguaje mediante el uso de comunicaciones oficiales anteriores o por medio del aporte de información sobre la estructura de las oficinas electorales podría dar lugar a la generación de datos de salida muy convincentes y aparentemente legítimos (Gupta et al., 2023).

Es probable que la IA exacerbe las ciberestafas basadas en texto, que son las más comunes, y que fomente nuevas formas de ciberestafa, como la imitación de voces y las llamadas telefónicas de altos funcionarios (Agencia de Seguridad Cibernética y Seguridad de la Infraestructura, 2024). Como resultado de intentos exitosos de ciberestafa los funcionarios electorales podrían divulgar datos confidenciales o dar acceso a los atacantes a sistemas clave, como los sitios web de los organismos electorales, las bases de datos de los votantes, los registros de datos o incluso los resultados de las elecciones.

Además, los organismos electorales que proporcionan plataformas donde los electores pueden presentar reclamos o solicitudes de información a los funcionarios pueden estar expuestos a recibir enormes cantidades de información generada por medio de la IA. Por ejemplo, los organismos electorales que cuentan con un sistema para que los votantes informen sobre problemas en los centros de votación pueden recibir reportes realistas pero falsos generados por la IA. Una avalancha de este tipo de informes podría sobrecargar los sistemas técnicos diseñados para procesar un número reducido de reclamos, impedir que se atiendan los problemas reales u ocasionar que los organismos electorales tomen decisiones basadas en información falsa.

3.4. **LOS CAMINOS A SEGUIR**

A continuación se presentan una serie de recomendaciones para que los organismos electorales y otros actores relevantes aborden algunos de los riesgos señalados en esta sección. Cabe destacar que en casi todos los casos los avances de la IA no hacen más que exacerbar las áreas de preocupación existentes para los organismos electorales y que los principales métodos de mitigación consisten en mejorar las actuales prácticas de seguridad.

1. Los organismos electorales deben trabajar en estrecha colaboración con el funcionariado local y con los grupos de interés comunitario para identificar la propagación de información falsa en torno a las elecciones. Además, los organismos electorales deben implementar métodos para reportar la información falsa sobre las elecciones ante otras autoridades y entidades gubernamentales.

2. Los organismos electorales deben tener una presencia verificada en las principales plataformas para combatir la propagación de información falsa y deben responder con rapidez en caso de detectar información falsa. Además, dichos los organismos deben difundir ampliamente contenidos exactos e informativos sobre las elecciones.

3. En caso de que ello forme parte de su mandato, los organismos electorales deben interactuar proactivamente con las principales plataformas de las redes sociales y de la IAG a fin de poner a disposición los recursos necesarios para refutar y desacreditar anticipadamente cualquier tipo de información falsa sobre las elecciones. También deben procurar que haya información electoral disponible en formato electrónico, para que las diversas plataformas puedan integrar fácilmente información correcta y exacta en los contenidos a ser difundidos entre sus usuarios.

4. Los organismos electorales deben trabajar en cooperación con otras entidades gubernamentales, como las autoridades reguladoras de comunicaciones y las agencias de ciberseguridad, para evitar la proliferación de desinformación y hacer que los responsables rindan cuentas. A tal fin, entre otras acciones, deben prevenir la suplantación de llamadas y números, y regular las llamadas robotizadas y el uso de *deepfakes* basados en IA en las redes de comunicación.

5. Los organismos electorales deben fortalecer las prácticas de ciberseguridad existentes mediante el uso de herramientas para prevenir ciberestafas, la capacitación del personal, la autenticación multifactorial y otras formas de colaboración con agencias y expertos en ciberseguridad. Además, dichos organismos deben exigir que los proveedores de tecnología electoral adopten medidas similares.

6. Los organismos electorales deben trabajar con las plataformas de IAG y exigir que rindan cuentas por sus acciones para evitar que sus herramientas se utilicen para difundir información falsa relacionada con las elecciones. Las medidas podrían incluir todo tipo de acciones, desde la regulación del uso y el desarrollo de las herramientas de la IAG hasta el suministro de información exacta a las diversas plataformas sobre la logística electoral. Los organismos electorales deben exigir a las plataformas de IAG que cuenten con normas transparentes que establezcan cómo se pueden utilizar sus herramientas para el desarrollo de actividades con fines políticos y cómo se garantizará el cumplimiento de esas normas.

7. Los organismos electorales deben exigir que las plataformas de las redes sociales rindan cuentas y deben garantizar que se tomen decisiones de moderación adecuadas de acuerdo con lo establecido por las normas y las leyes nacionales e internacionales.

8. Los organismos electorales deben informar a las organizaciones políticas sobre posibles amenazas relacionadas con la información y deben procurar que los partidos rindan cuentas por el uso que hagan de la IA. Exigir que el uso de la IA con fines políticos sea transparente y prohibir a las organizaciones políticas que difundan desinformación sobre la logística de las elecciones son algunas de las medidas que se podrían adoptar.

9. Los organismos electorales deberían considerar particularmente el impacto de la IA en todas estas estrategias de mitigación, y deberían centrarse particularmente en las comunidades marginadas, a las que se dirigen especialmente las campañas de desinformación y que son las más vulnerables a la persistencia de los sesgos que generan los modelos de IA.

Capítulo 4

MARCOS REGULATORIOS DE LA IA Y SU IMPACTO EN LAS ELECCIONES

El panorama jurídico en torno al uso de la IA sigue en desarrollo, y en distintos países se están considerando y aplicando una variedad de enfoques. En este capítulo se analizan brevemente algunos marcos regulatorios en materia de IA y se examina cómo podrían afectar el trabajo de las autoridades electorales.

El panorama jurídico en torno al uso de la IA sigue en desarrollo, y en distintos países se están considerando y aplicando una variedad de enfoques.

4.1. REGLAMENTO DE INTELIGENCIA ARTIFICIAL DE LA UNIÓN EUROPEA

El objetivo del Reglamento de Inteligencia Artificial de la Unión Europea[5] es regular el desarrollo y el uso de sistemas de IA en los Estados miembros de la Unión Europea. En marzo de 2024 el Parlamento Europeo aprobó dicho reglamento, que empezará a aplicarse gradualmente a partir de 2024 (Chee, 2024).

La mayoría de las investigaciones sobre el Reglamento de Inteligencia Artificial de la Unión Europea se centran en las implicaciones de la normativa para el sector privado, pero las normas también cubren el uso de la IA por parte de los gobiernos de la Unión Europea. En esta sección el foco se centra en las repercusiones normativas que este reglamento podría tener en el uso de sistemas de IA por parte de los organismos electorales y de otras autoridades electorales.

5 En el momento en que se redactó este informe el Reglamento de Inteligencia Artificial de la Unión Europea aún no había entrado en vigor. Por lo tanto, en este trabajo se ofrece una perspectiva preliminar de las posibles implicaciones de dicho reglamento para el uso de la IA por parte de los organismos electorales de los Estados miembros de la Unión Europea.

El Reglamento de Inteligencia Artificial se basa en los riesgos para establecer la regulación de los sistemas de IA, y clasifica los usos de la IA en función de cuatro niveles de riesgo: inaceptable, alto, bajo y mínimo.

Es probable que muchos usos de la IA para la gestión electoral correspondan a la categoría de alto riesgo.

Es probable que muchos usos de la IA para la gestión electoral correspondan a la categoría de alto riesgo, que abarca a los sistemas destinados a la administración de justicia y los procesos democráticos, incluidos los sistemas de IA destinados a ser utilizados para influir en el resultado de una elección o un referéndum, o en el comportamiento electoral de las personas físicas en el ejercicio de su voto en elecciones o referéndums, a excepción de los sistemas de IA a cuyos resultados de salida las personas no están directamente expuestas, como las herramientas utilizadas para organizar, optimizar y estructurar campañas políticas desde un punto de vista administrativo y logístico (Parlamento Europeo y Consejo de la Unión Europea, 2021, 40a).

Cabe señalar que el Reglamento de Inteligencia Artificial prohíbe el uso de los sistemas de IA que suponen un riesgo inaceptable (con algunas excepciones que responden, por ejemplo, a objetivos de seguridad nacional). En lo que respecta a los organismos electorales que utilizan y regulan la IA, esta prohibición comprende lo siguiente:

- el despliegue de técnicas subliminales, manipulativas o engañosas que puedan distorsionar el comportamiento y perjudicar la toma de decisiones con conocimiento de causa, ocasionando un daño significativo;

- la creación de bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales a partir de Internet o de imágenes de circuito cerrado de televisión, y

- la identificación biométrica remota en tiempo real en espacios de acceso público para garantizar el orden público (con algunas excepciones).

El Reglamento de Inteligencia Artificial regula sobre todo a los proveedores de sistemas de alto riesgo, que pueden ser proveedores de tecnología electoral o los propios organismos electorales. También regula a los denominados responsables del despliegue, entre los que se incluyen los organismos electorales que utilizan IA desarrollada tanto interna como externamente. En lo que respecta a los sistemas de alto riesgo, algunos de los requisitos que deben

cumplir los proveedores consisten en establecer sistemas de gestión de riesgos, garantizar la gobernanza de datos, facilitar la supervisión humana, y alcanzar niveles adecuados de exactitud, solidez y ciberseguridad. En lo que respecta a los responsables del desarrollo de sistemas de alto riesgo, algunos de los requisitos que deben cumplir son los siguientes: garantizar la supervisión humana realizada por personal competente, supervisar y operar el sistema de acuerdo con las instrucciones de uso, e informar a los proveedores sobre posibles problemas de funcionamiento (Parlamento Europeo y Consejo de la Unión Europea, 2021).

El marco basado en riesgos del Reglamento de Inteligencia Artificial puede ser de utilidad para que los organismos electorales exploren la posibilidad de aplicar la IA a los procesos electorales. Examinar la gravedad de los riesgos asociados a un determinado caso de uso de la IA (que, por ejemplo, podría afectar los resultados electorales o simplemente mejorar la eficiencia de un proceso existente) y adoptar las medidas propuestas para ese nivel de riesgo, incluido el análisis de la necesidad y la proporcionalidad de ese caso de uso, podría constituir un buen punto de partida. En lo que respecta a los sistemas de alto riesgo, los requisitos del Reglamento de Inteligencia Artificial —asegurar la supervisión humana, llevar a cabo auditorías de desempeño de los modelos y garantizar la gobernanza de datos— son clave para mitigar algunas de las preocupaciones asociadas al uso de la IA.

4.2. **ORDEN EJECUTIVA SOBRE IA DE ESTADOS UNIDOS**

Otra normativa potencialmente relevante es la Orden Ejecutiva sobre el Desarrollo y el Uso Seguro y Confiable de la Inteligencia Artificial del Gobierno de Estados Unidos [Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence] (Estados Unidos de América, 2023). La Orden Ejecutiva sobre IA abarca el uso de la IA por parte de las autoridades gubernamentales estadounidenses y, por lo tanto, podría repercutir en el uso de la IA para la gestión electoral en ese país. Concretamente, la Orden Ejecutiva sobre IA incluye disposiciones para:

- solicitar a las entidades federales que desarrollen y utilicen herramientas para verificar la autenticidad de las comunicaciones gubernamentales;

- evaluar y reforzar la forma en que las entidades federales adquieren y utilizan conjuntos de datos comerciales, y fortalecer las directrices en materia de privacidad;

- emitir normas para guiar el uso de la IA por parte de las entidades federales, y establecer pautas para proteger los derechos y la seguridad, y

- abordar las violaciones de los derechos y de las libertades civiles relacionadas con el uso de la IA en los sectores privado y público.

Cabe señalar que la Orden Ejecutiva sobre IA no es una ley estadounidense, sino una directiva ejecutiva que procura principalmente asignar recursos federales y clarificar aspectos relativos a la aplicación de las leyes vigentes en el contexto de la IA. Al igual que muchos otros países, Estados Unidos está debatiendo una ley general en materia de IA, similar al Reglamento de Inteligencia Artificial de la Unión Europea, que podría tener efectos adicionales en la labor de las autoridades electorales.

4.3. **NORMATIVA DEL TRIBUNAL SUPERIOR ELECTORAL DE BRASIL**

La normativa electoral recientemente adoptada por el Tribunal Superior Electoral de Brasil es potencialmente relevante (Conceição, 2024). Se trata de un ejemplo poco frecuente de una norma sobre IA diseñada específicamente a medida de las elecciones. La normativa, que principalmente se refiere al uso de la IA para desarrollar campañas políticas, contiene las siguientes disposiciones:

- las campañas electorales deben identificar claramente con una marca de agua todo el contenido de campaña generado por sistemas de IA;

- queda completamente prohibido el contenido fabricado o manipulado con el objetivo de divulgar información falsa;

- queda completamente prohibida la información falsa que pueda perjudicar la integridad electoral, y

- las campañas no pueden crear *deepfakes* ni *chatbots* para emular interacciones entre los candidatos y el público.

La normativa exige que las plataformas que alojen o difundan contenido electoral adopten medidas para evitar la propagación de cualquiera de las infracciones antes mencionadas.

4.4. **NORMATIVA SOBRE IA EN OTROS PAÍSES**

Otros países como Argentina, Canadá, Chile, Colombia, India, Japón, Nueva Zelanda, Perú o Singapur, entre otros, han aprobado directrices relacionadas con la IA o están elaborando normativas al respecto (Asociación Internacional de Profesionales de la Privacidad, 2024). Muchas de esas normativas adoptan enfoques basados en riesgos y se centran en los casos de uso de la IA de más alto riesgo tanto en el sector público como en el privado. Es probable que en muchos países gran parte de los casos de uso de la IA relacionados con los organismos electorales, así como muchos casos de uso de terceros con un impacto en los organismos electorales, entren en las categorías de más alto riesgo debido a su impacto potencial en la democracia.

Capítulo 5

CONCLUSIONES

En este informe se brinda un panorama general de las oportunidades y los retos relacionados con el uso de la IA para las elecciones. Se examina el potencial de los organismos electorales para utilizar la IA a fin de mejorar los procesos electorales a lo largo de todo el ciclo electoral, que incluye acciones como el registro de votantes, la planificación de las elecciones, la educación cívica, el seguimiento de las campañas y los medios de comunicación, las operaciones de votación, la supervisión de los centros de votación, la tabulación de los votos y el análisis de los resultados. Los organismos electorales que estén considerando realizar una rápida implementación de la IA también podrían contemplar el uso de herramientas de IA por parte de su personal, como Copilot de Microsoft, que podrían ser útiles para redactar o resumir correos electrónicos y contenidos.

Si bien muchos de estos casos de uso son prometedores, todos conllevan riesgos.

Si bien muchos de estos casos de uso son prometedores, todos conllevan riesgos. En la práctica las dificultades técnicas para implementar, supervisar y mantener algunos sistemas de IA, así como la falta de confiabilidad de muchos modelos, plantean serias dudas acerca de la capacidad de los organismos electorales para utilizar y gestionar la IA y mantener al mismo tiempo la integridad electoral. Los riesgos relativos a la confiabilidad pueden tener implicaciones éticas, ya que el uso de la IA puede dar lugar a prejuicios y discriminación, que afectan especialmente a las comunidades más vulnerables. El uso de la IA puede reducir la confianza del público en las elecciones, sobre todo cuando requiere una mayor vigilancia, lo que puede tener un efecto negativo en los derechos humanos.

Los organismos electorales que estén considerando la posibilidad de usar la IA deben centrarse en los principios de necesidad,

minimización de datos y proporcionalidad, y deben prestar especial atención a los riesgos y los beneficios de utilizar la IA en reemplazo de las prácticas existentes. La aplicación de normas estrictas de transparencia, ciberseguridad, control, auditoría y supervisión humana puede contribuir a atenuar algunos de los riesgos que genera el uso de la IA. Sin embargo, los organismos electorales que estén considerando su utilización deberían centrarse en un principio en los casos de uso que presentan los menores riesgos potenciales. En casi todos los casos, los organismos electorales deberían centrarse primero en el desarrollo de la infraestructura, de los conocimientos técnicos y de las prácticas éticas y de auditoría necesarias para lograr un uso seguro de la IA, antes de adquirir o desarrollar esta tecnología.

Respecto del uso de la IA por parte de actores distintos de los organismos electorales, es fundamental que estos elaboren planes para responder a las diferentes formas en que la IA podría afectar a la gestión electoral. Por ejemplo, es probable que los organismos electorales enfrenten un aumento tanto de la cantidad como de la calidad de la información falsa relacionada con las elecciones. Si bien es posible que la IA no altere drásticamente el desarrollo de información falsa, podría socavar aún más la confianza en los procesos electorales, por lo que los organismos electorales deben tomar medidas para combatir la desinformación, especialmente aquella dirigida a las comunidades más vulnerables. Para lograrlo los organismos electorales tienen que trabajar junto con el funcionariado local, los grupos comunitarios, las empresas de IAG y las plataformas de las redes sociales.

Es probable que las organizaciones y las campañas políticas utilicen la IA para influir en las elecciones a través de la generación de contenidos y de publicidad, el análisis de datos y otras acciones de campaña. Los organismos electorales que como parte de su mandato deben supervisar a las organizaciones políticas tienen que trabajar junto con otras entidades gubernamentales para limitar la desinformación durante las campañas, exigir marcas de agua en todo el contenido generado mediante IA y reflexionar sobre los efectos que tiene en la privacidad el uso de la IA durante las campañas.

Los organismos electorales deben ser conscientes de las crecientes amenazas a la ciberseguridad que supone la IA, ya sea que la utilicen los propios organismos electorales u otros actores externos. Los organismos electorales deben estar preparados sobre todo para

hacer frente a los intentos de ciberestafa (*phishing)* de calidad superior que utilizan la IAG para manipular a las personas a fin de que compartan información interna. Algunas de las medidas que vale la pena considerar consisten en trabajar en estrecha colaboración con expertos en ciberseguridad, seguir las prácticas de ciberseguridad existentes recomendadas y capacitar al personal sobre estas amenazas.

Además, los organismos electorales deben trabajar en estrecha colaboración con sus gobiernos para comprender las implicaciones de los distintos marcos regulatorios y conocer cómo pueden afectar el trabajo de dichos organismos. Por ejemplo, los casos de uso desplegados por los organismos electorales que estén considerando la utilización de la IA en la Unión Europea podrían entrar en la categoría de alto riesgo, lo que significa que tendrán que cumplir con normas de transparencia, rendición de cuentas y supervisión humana más estrictas que las que requiere la implementación de otras tecnologías. Es posible que los organismos electorales tengan que modificar sus propios mandatos y estructuras regulatorias para preservar su capacidad de garantizar la integridad electoral.

Por último, dado que la IA y la correspondiente normativa constituyen campos en rápida evolución, los organismos electorales deben considerar que la información brindada en este informe ofrece un panorama general y no exhaustivo del papel que podría desempeñar la IA en las elecciones. Estos organismos deben mantenerse informados sobre el desarrollo, las oportunidades y los riesgos de la IA y deben promover una estrecha colaboración con expertos gubernamentales y no gubernamentales para actualizar continuamente sus conocimientos y su comprensión del contexto. El objetivo de este informe es brindar un punto de partida para analizar el uso de la IA por parte de los organismos electorales y examinar sus posibles implicaciones.

Bibliografía

Agencia de Seguridad Cibernética y Seguridad de la Infraestructura (CISA), "Enfoque basado en riesgos: IA generativa y el ciclo electoral de 2024", 18 de enero de 2024, <https://www.cisa.gov/resources-tools/resources/risk-focus-generative-ai-and-2024-election-cycle>, fecha de consulta: 15 de abril de 2024.

Akbar, P., Loilatu, M. J., Pribadi, U. y Sudiar, S., "Implementation of artificial intelligence by the General Elections Commission in creating a credible voter list" [Uso de la inteligencia artificial por parte de la Comisión de Elecciones Generales para crear una lista de votantes creíble], *IOP Conference Series. Earth and Environmental Science*, 717/012017 (2021), <https://doi.org/10.1088/1755-1315/717/1/012017>.

Al-Haidary, M., Ajlouni, M. A., Talib, M. A., Abbas, S., Nasir, Q. y Basaeed, E., "Metaheuristic approaches to facility location problems: A systematic review" [Enfoques metaheurísticos de los problemas de localización de instalaciones: una revisión sistemática], en Instituto de Ingenieros Eléctricos y Electrónicos, *2021 4th International Conference on Signal Processing and Information Security (ICSPIS)* [Cuarta Conferencia Internacional sobre Procesamiento de Señales y Seguridad de la Información (ICSPIS) 2021] (Instituto de Ingenieros Eléctricos y Electrónicos, 2021), págs. 49-52, <https://doi.org/10.1109/ICSPIS53734.2021.9652430>.

Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A. y Rieke, A., "Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes" [Discriminación a través de la optimización: cómo la distribución de anuncios de Facebook puede generar resultados sesgados], arXiv, 12 de septiembre de 2019, <https://doi.org/10.48550/arXiv.1904.02095>.

Asociación Internacional de Profesionales de la Privacidad (IAPP), "Global AI law and policy tracker" [Rastreador mundial de leyes y políticas sobre IA], febrero de 2024, <https://iapp.org/resources/article/global-ai-legislation-tracker>, fecha de consulta: 15 de abril de 2024.

Barretto, S., Chown, W., Meyer, D., Soni, A., Tata, A. y Halderman, J. A., "Improving the accuracy of ballot scanners using supervised learning" [Mejorar la exactitud de los escáneres de boletas mediante el aprendizaje supervisado], en R. Krimmer, M. Volkamer, D. Duenas-Cid, O. Kulyk, P. Rønne, M. Solvak y M. Germann (eds.), *Electronic Voting: 6th International Joint Conference, E-Vote-ID 2021, Virtual Event, October 5-8, 2021, Proceedings* [Votación electrónica: 6.ª Conferencia Internacional Conjunta, E-Vote-ID 2021, evento virtual, 5 al 8 de octubre de 2021, memoria] (Springer International Publishing, 2021), págs. 17-32, <https://doi.org/10.1007/978-3-030-86942-7_2>.

Bender, S. M. L., "Algorithmic elections" [Elecciones algorítmicas], *Michigan Law Review*, 121/3 (2022), págs. 489-524, <https://doi.org/10.36644/mlr.121.3.algorithmic>.

Bicu, I., "The information environment around elections" [El entorno informativo de las elecciones], IDEA Internacional, 2023, <https://www.idea.int/theme/information-communication-and-technology-electoral-processes/information-environment-around-elections>, fecha de consulta: 15 de abril de 2024.

Bond, S., "AI fakes raise election risks as lawmakers and tech companies scramble to catch up" [Las noticias falsas generadas con IA aumentan los riesgos electorales mientras los legisladores y las empresas tecnológicas luchan por ponerse al día], NPR, 8 de febrero de 2024, <https://www.npr.org/2024/02/08/1229641751/ai-deepfakes-election-risks-lawmakers-tech-companies-artificial-intelligence>, fecha de consulta: 15 de abril de 2024.

Brynjolfsson, E., Li, D. y Raymond, L. R., "Generative AI at Work" [La IA generativa en el trabajo], documento de trabajo núm. 31161, Oficina Nacional de Investigación Económica, noviembre de 2023, <https://doi.org/10.3386/w31161>.

Calma, J., "NYC Mayor Eric Adams uses AI to make robocalls in languages he doesn't speak" [El alcalde de Nueva York, Eric Adams, utiliza la IA para hacer llamadas robotizadas en idiomas que él no habla], The Verge, 17 de octubre de 2023, <https://www.theverge.com/2023/10/17/23920733/nyc-mayor-eric-adams-ai-robocalls-spanish-mandarin>, fecha de consulta: 15 de abril de 2024.

Carrasco, M., Habib, C., Felden, F., Sargeant, R., Mills, S., Shenton, S., Ingram, J. y Dando, G., "Generative AI for the public sector: The journey to scale" [La IA generativa para el sector público: el camino para extender su uso], Boston Consulting Group, 26 de marzo de 2024, <https://www.bcg.com/publications/2024/gen-ai-journey-to-scale-in-government>, fecha de consulta: 15 de abril de 2024.

Centro de Información de Registro Electrónico (ERIC), "Technology and security brief – v6.1" [Informe sobre tecnología y seguridad - versión 6.1], 8 de marzo de 2024, <https://ericstates.org/wp-content/uploads/documents/ERIC-Tech-Security-Brief.pdf>, fecha de consulta: 15 de abril de 2024.

Centro Nacional de Ciberseguridad (NCSC), "The near-term impact of AI on the cyber threat" [El impacto a corto plazo de la IA en la amenaza cibernética], 24 de enero de 2024, <https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>, fecha de consulta: 15 de abril de 2024.

Chee, F. Y., "Europe one step away from landmark AI rules after lawmakers' vote" [Europa a un paso de normas clave sobre IA tras la votación de los legisladores], Reuters, 14 de marzo de 2024, <https://www.reuters.com/technology/eu-lawmakers-endorse-political-deal-artificial-intelligence-rules-2024-03-13>, fecha de consulta: 15 de abril de 2024.

Clark, A., "The cost of democracy: The determinants of spending on the public administration of elections" [El costo de la democracia: los factores determinantes del gasto en la administración pública de las elecciones], *International Political Science Review*, 40/3 (2019), págs. 354-369, <https://doi.org/10.1177/0192512118824787>.

Comisión Interamericana de Derechos Humanos (CIDH), *Standards for a Free, Open and Inclusive Internet* [Estándares para una Internet libre, abierta e inclusiva], OEA/Ser.L/V/II, OEA, 15 de marzo de 2017, <https://www.oas.org/en/iachr/expression/docs/publications/internet_2016_eng.pdf>, fecha de consulta: 15 de abril de 2024.

Conceição, L. H. M., "Brazilian judges regulate elections… and AI" [Los jueces brasileños regulan las elecciones… y la IA], Verfassungsblog, 15 de marzo de 2024, <https://doi.org/10.59704/612f31a89ce38fc6>.

Crawford, K., *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence* [Atlas de la IA: poder, política y costos planetarios de la inteligencia artificial] (New Haven, CT: Yale University Press, 2022), <https://doi.org/10.12987/9780300252392>.

Deepak, P., Simoes, S. y MacCarthaigh, M., "AI and core electoral processes: Mapping the horizons" [La IA y los principales procesos electorales: trazar los horizontes], *AI Magazine*, 44/3 (2023), págs. 218-239, <https://doi.org/10.1002/aaai.12105>.

Dhiman, P., Kaur, A., Iwendi, C. y Mohan, S. K., "A scientometric analysis of deep learning approaches for detecting fake news" [Un análisis cienciométrico de los enfoques de aprendizaje profundo para detectar noticias falsas], *Electronics*, 12/4 (2023), pág. 948, <https://doi.org/10.3390/electronics12040948>.

Dommett, K., "Data-driven political campaigns in practice: Understanding and regulating diverse data-driven campaigns" [Campañas políticas basadas en datos en la práctica: comprender y regular distintas campañas basadas en datos], *Internet Policy Review*, 8/4 (2019), <https://doi.org/10.14763/2019.4.1432>.

Eisen, N., Turner Lee, N., Galliher, C. y Katz, J., "AI can strengthen U.S. democracy—and weaken it" [La IA puede fortalecer la democracia estadounidense, y debilitarla], Brookings, 21 de noviembre de 2023, <https://www.brookings.edu/articles/ai-can-strengthen-u-s-democracy-and-weaken-it>, fecha de consulta: 15 de abril de 2024.

Estados Unidos de América, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" [Orden ejecutiva sobre el desarrollo y el uso seguro y confiable de la inteligencia artificial], La Casa Blanca, 30 de octubre de 2023, <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>, fecha de consulta: 15 de abril de 2024.

Goel, S., Meredith, M., Morse, M., Rothschild, D. y Shirani-Mehr, H., "One person, one vote: Estimating the prevalence of double voting in U.S. presidential elections" [Una persona, un voto: estimación de la prevalencia del voto doble en las elecciones presidenciales de Estados Unidos], *American Political Science Review*, 114/2 (2020), págs. 456-469, <https://doi.org/10.1017/S000305541900087X>.

Green, J., "Anomaly detection in election data and its representation of U.S. infrastructure vulnerability" [La detección de anomalías en los datos electorales y su representación de la vulnerabilidad de la infraestructura de Estados Unidos], en Instituto de Ingenieros Eléctricos y Electrónicos, *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* [12.ª Conferencia Anual de Tecnologías de la Información, Electrónica y Comunicaciones Móviles 2021] (Instituto de Ingenieros Eléctricos y Electrónicos, 2021), págs. 503-508, <https://doi.org/10.1109/IEMCON53756.2021.9623111>.

Gstrein, O. J., Bunnik, A. y Zwitter, A., "Ethical, legal and social challenges of predictive policing" [Desafíos éticos, legales y sociales de la vigilancia policial predictiva], *Católica Law Review: Direito Penal*, 3/3 (2019), págs. 77-98, <https://papers.ssrn.com/abstract=3447158>, fecha de consulta: 15 de abril de 2024.

Gupta, M., Akiri, C., Aryal, K., Parker, E. y Praharaj, L., "From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy" [Del ChatGPT al ThreatGPT: el impacto de la IA generativa en la ciberseguridad y la privacidad], *IEEE Access*, 11 (2023), págs. 80218-80245, <https://doi.org/10.1109/ACCESS.2023.3300381>.

Haenschen, K., "The conditional effects of microtargeted Facebook advertisements on voter turnout" [Los efectos condicionales de los anuncios de Facebook para audiencias microsegmentadas sobre la participación electoral], *Political Behavior*, 45/1 (2022), págs. 1661-1681, <https://doi.org/10.1007/s11109-022-09781-7>.

Hajnal, Z., Kuk, J. y Lajevardi, N., "We all agree: Strict voter ID laws disproportionately burden minorities" [Estamos todos de acuerdo: las estrictas leyes de identificación de votantes afectan de manera desigual a las minorías], *The Journal of Politics*, 80/3 (2018), págs. 1052-1059, <https://doi.org/10.1086/696617>.

Hardyns, W. y Rummens, A., "Predictive policing as a new tool for law enforcement? Recent developments and challenges" [¿La vigilancia policial predictiva como nueva herramienta para la aplicación de la ley? Desarrollos recientes y desafíos], *European Journal on Criminal Policy and Research*, 24/3 (2018), págs. 201-218, <https://doi.org/10.1007/s10610-017-9361-2>.

Hsu, T., "New Hampshire officials to investigate A.I. robocalls mimicking Biden" [Las autoridades de New Hampshire investigan llamadas robotizadas basadas en IA en que se imita a Biden], *The New York Times*, 22 de enero de 2024, <https://www.nytimes.com/2024/01/22/business/media/biden-robocall-ai-new-hampshire.html>, fecha de consulta: 15 de abril de 2024.

Hsu, T., Thompson, S. A. y Myers, S. L., "Elections and disinformation are colliding like never before in 2024" [Las elecciones y la desinformación chocan como nunca antes en 2024], *The New York Times*, 9 de enero de 2024, <https://www.nytimes.com/2024/01/09/business/media/election-disinformation-2024.html>, fecha de consulta: 15 de abril de 2024.

Hussain, R., Raza, A., Siddiqi, I., Khurshid, K. y Djeddi, C., "A comprehensive survey of handwritten document benchmarks: Structure, usage and evaluation" [Un estudio exhaustivo de las marcas de los documentos manuscritos: estructura, uso y evaluación], *EURASIP Journal on Image and Video Processing*, 1 (2015), <https://doi.org/10.1186/s13640-015-0102-5>.

Juneja, P. y Floridi, L., "Using Twitter to detect polling place issues on U.S. election days" [El uso de Twitter para detectar problemas en los lugares de votación durante las elecciones en Estados Unidos], SSRN, 24 de enero de 2023, <https://doi.org/10.2139/ssrn.4334243>.

Jungherr, A., "Artificial intelligence and democracy: A conceptual framework" [Inteligencia artificial y democracia: un marco conceptual], *Social Media + Society*, 9/3 (2023), <https://doi.org/10.1177/20563051231186353>.

Jungherr, A. y Rauchfleisch, A., "Negative downstream effects of alarmist disinformation discourse: Evidence from the United States" [Los efectos negativos del discurso alarmista sobre la desinformación: evidencia de los Estados Unidos], *Political Behavior* (2024), <https://doi.org/10.1007/s11109-024-09911-3>.

Kan, H. J., Kharrazi, H., Chang. H. Y., Bodycombe, D., Lemke, K. y Weiner, J. P., "Exploring the use of machine learning for risk adjustment: A comparison of standard and penalized linear regression models in predicting health care costs in older adults" [Exploración del uso del aprendizaje automático para el ajuste del riesgo: una comparación de modelos de regresión lineal estándar y con penalización para la predicción de los costos de atención médica de personas mayores], *PloS One*, 14/3 (2019), <https://doi.org/10.1371/journal.pone.0213258>.

Kennedy, R., Wojcik, S. y Lazer, D., "Improving election prediction internationally" [Mejorar la predicción electoral a escala internacional], *Science*, 355/6324 (2017), págs. 515-520, <https://www.science.org/doi/10.1126/science.aal2887>.

Kondamudi, M. R., Sahoo, S. R., Chouhan, L. y Yadav, N., "A comprehensive survey of fake news in social networks: Attributes, features, and detection approaches" [Un estudio exhaustivo de las noticias falsas en redes sociales: atributos, características y enfoques de detección], *Journal of King Saud University - Computer and Information Sciences*, 35/6 (2023), <https://doi.org/10.1016/j.jksuci.2023.101571>.

Kwon, C., Moreno, A. y Raman, A., "The impact of input inaccuracy on leveraging AI tools: Evidence from algorithmic labor scheduling" [El impacto de la inexactitud de los datos de entrada en el aprovechamiento de las herramientas de la IA: evidencia de la programación algorítmica del trabajo], SSRN, 22 de octubre de 2023, <https://doi.org/10.2139/ssrn.4602747>.

Landemore, H., "Fostering more inclusive democracy with AI" [Promover una democracia más inclusiva con la IA], Fondo Monetario Internacional, diciembre de 2023, <https://www.imf.org/en/Publications/fandd/issues/2023/12/POV-Fostering-more-inclusive-democracy-with-AI-Landemore>, fecha de consulta: 15 de abril de 2024.

Liu, Z. y Hu, S., "Predicting the fundraising performance of environmental crowdfunding projects: An interpretable machine learning approach" [Predicción del desempeño de la recaudación de fondos de proyectos ambientales de microfinanciación colectiva: un enfoque de aprendizaje automático interpretable], *Information Processing & Management*, 61/2 (2024), <https://doi.org/10.1016/j.ipm.2023.103587>.

Livemint, "EC to start campaign to link voter ID with Aadhaar from August 1. Check details here" [La CE iniciará la campaña para vincular el documento de identidad de los votantes con Aadhaar a partir del 1 de agosto. Consulte los detalles aquí], *Mint*, 25 de julio de 2022, <https://www.livemint.com/news/india/ec-to-start-campaign-to-link-voter-id-with-aadhaar-from-august-1-check-details-here-11658748573098.html>, fecha de consulta: 15 de abril de 2024.

Mann, C. y Stein, R. M., "The impact of polling places on voting" [El impacto de los recintos electorales en la votación], ponencia preparada para la Conferencia sobre la Administración y Reforma de la Ciencia Electoral, Universidad de Pensilvania, julio de 2019, <https://web.sas.upenn.edu/esra2019/files/2019/07/Mann-and-Stein-Polling-Place-Effect.pdf>, fecha de consulta: 15 de abril de 2024.

Markay, L., "AI becomes a political 'super-weapon'" [La IA se convierte en una "superarma" política], Axios, 7 de octubre de 2022, <https://www.axios.com/2022/10/07/ai-becomes-a-political-super-weapon>, fecha de consulta: 15 de abril de 2024.

MIT Election Lab [Laboratorio de Elecciones del MIT], "Voting technology" [Tecnología electoral], 21 de abril de 2023, <https://electionlab.mit.edu/research/voting-technology>, fecha de consulta: 15 de abril de 2024.

Mökander, J. y Floridi, L., "Ethics-based auditing to develop trustworthy AI" [La auditoría ética para desarrollar una IA confiable], *Minds and Machines*, 31/2 (2021), págs. 323-327, <https://doi.org/10.1007/s11023-021-09557-8>.

Moses, L. y Box-Steffensmeier, J. M., "Considerations for machine learning use in political research with application to voter turnout" [Reflexiones sobre el uso del aprendizaje automático en la investigación política aplicada a la participación electoral], 2021, <https://polmeth.theopenscholar.com/files/polmeth/files/moses-box-steffensmeier-2020.pdf>, fecha de consulta: 15 de abril de 2024.

Mughal, N., "Deepfakes, Internet access cuts make election coverage hard, journalists say" [*Deepfakes* y cortes en el acceso a Internet dificultan la cobertura de las elecciones, según los periodistas], Voice of America, 22 de febrero de 2024, <https://www.voanews.com/a/deepfakes-internet-access-cuts-make-election-coverage-hard-journalists-say-/7498917.html>, fecha de consulta: 15 de abril de 2024.

Muppasani, B., Pallagani, V., Lakkaraju, K., Lei, S., Srivastava, B., Robertson, B., Hickerson, A. y Narayanan, V., "On safe and usable chatbots for promoting voter participation" [*Chatbots* seguros y fáciles de usar para promover la participación electoral], *AI Magazine*, 44/3 (2023), págs. 240-247, <https://doi.org/10.1002/aaai.12109>.

Naciones Unidas, "La desinformación y la libertad de opinión y de expresión. Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Irene Khan", A/HRC/47/25, Consejo de Derechos Humanos, Asamblea General de las Naciones Unidas, 13 de abril de 2021, <https://www.ohchr.org/es/documents/reports/disinformation-and-freedom-opinion-and-expression-report-special-rapporteur>, fecha de consulta: 15 de abril de 2024.

Norden, L. y Ramachandran, G., "Artificial intelligence and election security" [Inteligencia artificial y seguridad electoral], Brennan Center for Justice, 5 de octubre de 2023, <https://www.brennancenter.org/our-work/research-reports/artificial-intelligence-and-election-security>, fecha de consulta: 15 de abril de 2024.

Noy, S. y Zhang, W., "Experimental evidence on the productivity effects of generative artificial intelligence" [Evidencia experimental sobre los efectos en la productividad de la inteligencia artificial generativa], *Science*, 381/6654 (2023), págs. 187-192, <https://www.science.org/doi/10.1126/science.adh2586>.

OpenAI, "How OpenAI is approaching 2024 worldwide elections" [Cómo OpenAI aborda las elecciones mundiales de 2024] [blog], 15 de enero de 2024, <https://openai.com/blog/how-openai-is-approaching-2024-worldwide-elections> [última actualización: 14 de mayo de 2024], fecha de consulta: 15 de abril de 2024.

Organización para la Cooperación y el Desarrollo Económicos (OCDE), Recomendación sobre la inteligencia artificial (traducción no oficial), OECD/LEGAL/0449, 21 de mayo de 2019, <https://legalinstruments.oecd.org/api/download/?uri=/public/db5053b5-93e0-4cf5-a7cf-edce5ee6e893.pdf>, fecha de consulta: 15 de abril de 2024.

Parkin, B. y Bokhari, F., "Imran Khan taps AI and TikTok to fight Pakistan election from jail" [Imran Khan recurre a la IA y a TikTok para participar en las elecciones de Pakistán desde la cárcel], *Financial Times*, 1 de febrero de 2024, <https://www.ft.com/content/7c3c5827-c965-453c-8bd1-d1312e90669a>, fecha de consulta: 15 de abril de 2024.

Parlamento Europeo y Consejo de la Unión Europea, Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts [Propuesta de Reglamento del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión], 2021/0106 (COD), 21 de abril de 2021, <https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-FullText.pdf>, fecha de consulta: 15 de abril de 2024.

Pech, L., "The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU" [El concepto del efecto de desaliento: su desaprovechado potencial para proteger mejor la democracia, el Estado de Derecho y los derechos fundamentales en la Unión Europea], Open Society European Policy Institute, marzo de 2021, <https://www.opensocietyfoundations.org/uploads/c8c58ad3-fd6e-4b2d-99fa-d8864355b638/the-concept-of-chilling-effect-20210322.pdf>, fecha de consulta: 15 de abril de 2024.

Perkowitz, S., "The bias in the machine: Facial recognition technology and racial disparities" [El sesgo en la máquina: tecnología de reconocimiento facial y desigualdades raciales], *MIT Case Studies in Social and Ethical Responsibilities of Computing* [Estudios de caso del MIT sobre las responsabilidades sociales y éticas en la informática], invierno (2021), <https://doi.org/10.21428/2c646de5.62272586>.

Rawte, V., Sheth, A. y Das, A., "A survey of hallucination in 'large' foundation models" [Un estudio sobre la alucinación en los "grandes" modelos fundacionales], arXiv, 12 de septiembre de 2023, <https://doi.org/10.48550/arXiv.2309.05922>.

Rayda, N., "Indonesia elections 2024: How AI has become a double-edged sword for candidates and election officials" [Elecciones en Indonesia en 2024: cómo la IA se ha convertido en un arma de doble filo para los candidatos y los funcionarios electorales], CNA, 4 de febrero de 2024, <https://www.channelnewsasia.com/asia/ai-disinformation-deepfakes-indonesia-elections-4091296>, fecha de consulta: 15 de abril de 2024.

Richardson, R., Schultz, J. y Crawford, K., "Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice" [Datos sucios, malas predicciones: cómo las violaciones de los derechos civiles afectan los datos policiales, los sistemas de vigilancia policial predictiva y la justicia], *New York University Law Review Online*, 94/192 (2019), <https://papers.ssrn.com/abstract=3333423>, fecha de consulta: 15 de abril de 2024.

Simchon, A., Edwards, M. y Lewandowsky, S., "The persuasive effects of political microtargeting in the age of generative artificial intelligence" [Los efectos persuasivos de los anuncios políticos dirigidos a audiencias microsegmentadas en la era de la inteligencia artificial generativa], *PNAS Nexus*, 3/2 (2024), pág. 35, <https://doi.org/10.1093/pnasnexus/pgae035>.

Solender, A. y Fried, I., "Scoop: Congress bans staff use of Microsoft's AI Copilot" [Primicia: el Congreso prohíbe al personal utilizar AI Copilot de Microsoft], Axios, 29 de marzo de 2024, <https://www.axios.com/2024/03/29/congress-house-strict-ban-microsoft-copilot-staffers>, fecha de consulta: 15 de abril de 2024.

Stokel-Walker, C., "AI chatbot models 'think' in English even when using other languages" [Los modelos de *chatbot* de IA "piensan" en inglés incluso cuando utilizan otros idiomas], *New Scientist*, 8 de marzo de 2024, <https://www.newscientist.com/article/2420973-ai-chatbot-models-think-in-english-even-when-using-other-languages>, fecha de consulta: 15 de abril de 2024.

Suhenda, D., "KPU insists on using Sirekap" [KPU insiste en utilizar Sirekap], *The Jakarta Post*, 22 de febrero de 2024, <https://www.thejakartapost.com/indonesia/2024/02/22/kpu-insists-on-using-sirekap.html>, fecha de consulta: 15 de abril de 2024.

Talarico, L. y Maya Duque, P. A., "An optimization algorithm for the workforce management in a retail chain" [Un algoritmo de optimización para la gestión de la mano de obra en una cadena minorista], *Computers & Industrial Engineering*, 82 (2015), págs. 65-77, <https://doi.org/10.1016/j.cie.2015.01.014>.

Üçoğlu, D., "Current machine learning applications in accounting and auditing" [Aplicaciones actuales del aprendizaje automático en contabilidad y auditoría], *Pressacademia*, 12/1 (2020), págs. 1-7, <https://doi.org/10.17261/Pressacademia.2020.1337>.

Valle-Cruz, D., Fernández-Cortez, V. y Gil-García, J. R., "From e-budgeting to smart budgeting: Exploring the potential of artificial intelligence in government decision-making for resource allocation" [Del presupuesto electrónico al presupuesto inteligente: exploración del potencial de la inteligencia artificial en la toma de decisiones gubernamentales para la asignación de recursos], *Government Information Quarterly*, 39/2 (2022), <https://doi.org/10.1016/j.giq.2021.101644>.

Van Brakel, R., "Pre-emptive big data surveillance and its (dis)empowering consequences: The case of predictive policing" [La vigilancia anticipada de macrodatos y sus consecuencias (des)empoderadoras: el caso de la vigilancia policial predictiva], en B. van der Sloot, D. Broeders y E. Schrijvers (eds.), *Exploring the Boundaries of Big Data* [Explorar los límites de los macrodatos] (Ámsterdam: Amsterdam University Press, 2016), págs. 117-141, <https://doi.org/10.2139/ssrn.2772469>.

Van der Staak, S. y Wolf, P., *Cybersecurity in Elections: Models of Interagency Collaboration* [Ciberseguridad en las elecciones: modelos de colaboración interinstitucional] (Estocolmo: IDEA Internacional, 2019), <https://doi.org/10.31752/idea.2019.23>.

Vandewalker, I., "Digital Disinformation and Vote Suppression" [Desinformación digital y supresión de votos], Brennan Center for Justice, 2 de septiembre de 2020, <https://www.brennancenter.org/our-work/research-reports/digital-disinformation-and-vote-suppression>, fecha de consulta: 15 de abril de 2024.

Varna, A., "Big data analytics and transformation of election campaign in India" [Análisis de macrodatos y transformación de la campaña electoral en India], Proceedings of the 2nd International Conference on Information Systems & Management Science (ISMS) 2019 [Actas de la 2.ª Conferencia Internacional sobre Sistemas de Información y Ciencias de la Gestión (ISMS) 2019], Universidad de Tripura, 30 de diciembre de 2019, <https://doi.org/10.2139/ssrn.3511428>.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L. y Polosukhin, I., "Attention is all you need" [Solo necesitas atención], arXiv, 6 de diciembre de 2017, <http://arxiv.org/abs/1706.03762>, fecha de consulta: 15 de abril de 2024.

Wei, A., Haghtalab, N. y Steinhardt, J., *Jailbroken: How does LLM safety training fail?* [*Jailbroken*: ¿en qué falla la formación en seguridad de los LLM?], arXiv, 5 de julio de 2023, <https://doi.org/10.48550/arXiv.2307.02483>.

Wolf, P., Alim, A., Kasaro, B., Saneem, M., Namugera, P. y Zorigt, T., *Introducing Biometric Technology in Elections* [Introducción de la tecnología biométrica en las elecciones] (Estocolmo: IDEA Internacional, 2017), <https://www.idea.int/publications/catalogue/introducing-biometric-technology-elections>, fecha de consulta: 15 de abril de 2024.

Yamin, K., Jadali, N., Xie, Y. y Nazzal, D., "Novelty detection for election fraud: A case study with agent-based simulation data" [Detección de novedades en el fraude electoral: un estudio de caso con datos de simulación basados en agentes], *AI Magazine*, 44/3 (2023), págs. 255-262, <https://doi.org/10.1002/aaai.12112>.

Zhang, M., Álvarez, R. M. y Levin, I., "Election forensics: Using machine learning and synthetic data for possible election anomaly detection" [Análisis forense de las elecciones: uso del aprendizaje automático y de datos sintéticos para la detección de posibles anomalías electorales], *Plos One*, 14/10 (2019), <https://doi.org/10.1371/journal.pone.0223950>.

Zhao, F., Zhang, C., Saxena, N., Wallach, D., Shahariar, A. y Rabby, A., "Ballot tabulation using deep learning" [Tabulación de los votos mediante el aprendizaje profundo], en Instituto de Ingenieros Eléctricos y Electrónicos, *2023 IEEE 24th International Conference on Information Reuse and Integration for Data Science (IRI)* [24.ª Conferencia Internacional sobre Reutilización de la Información e Integración de Datos para la Ciencia de Datos 2023] (Instituto de Ingenieros Eléctricos y Electrónicos, 2023), págs. 107-114, <https://doi.org/10.1109/IRI58017.2023.00026>.

Zhou, J., Zhang, Y., Luo, Q., Parker, A. G. y De Choudhury, M., "Synthetic lies: Understanding AI-generated misinformation and evaluating algorithmic and human solutions" [Mentiras sintéticas: comprender la información falsa generada por la IA y evaluar soluciones algorítmicas y humanas], en *CHI'23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* [Memoria de la conferencia CHI de 2023 sobre los factores humanos en los sistemas informáticos] (Nueva York: Asociación para la Maquinaria Computacional, 2023), págs. 1-20, <https://doi.org/10.1145/3544548.3581318>.

Zhuang, Y., "Imran Khan's 'victory speech' from jail shows A.I.'s peril and promise" [El "discurso de la victoria" de Imran Khan desde la cárcel muestra el peligro y la promesa de la IA], *The New York Times*, 11 de febrero de 2024, <https://www.nytimes.com/2024/02/11/world/asia/imran-khan-artificial-intelligence-pakistan.html>, fecha de consulta: 15 de abril de 2024.

Anexo A. Términos clave

A continuación se definen algunos términos técnicos y no técnicos relacionados con la IA, que se utilizan en este informe. El objetivo no es brindar definiciones exhaustivas, sino contribuir a la comprensión del texto por parte de los lectores.

Término	Explicación
Ajuste y aprendizaje por transferencia	Es un proceso por medio del cual los modelos de aprendizaje profundo pueden especializarse en una tarea específica al mismo tiempo en que mantienen los conocimientos de su entrenamiento inicial. Por ejemplo, se puede utilizar un LLM para el fin específico de clasificar las publicaciones en redes sociales referidas a las elecciones mediante su ajuste a partir de un conjunto de datos etiquetados para definir dos grupos: las publicaciones que no hablan de las elecciones y aquellas que sí hablan de las elecciones.
Alucinación de modelos de lenguaje de gran tamaño (LLM)	Describe la tendencia de muchos LLM que inventan información en respuesta a consultas de texto.
Aprendizaje automático	Describe los métodos técnicos desarrollados más recientemente, como las redes neuronales, los transformadores y los métodos de *boosting* y *bagging*. En muchos casos estos métodos se utilizan para fines predictivos, lo que implica tomar decisiones basadas en datos más que explicar datos anteriores.
Aprendizaje no supervisado	Describe un subconjunto del aprendizaje automático en que los datos de entrenamiento no están etiquetados y el objetivo del modelo es encontrar patrones en los datos. Un ejemplo sería el desarrollo de un modelo que agrupe muestras de escritura similares.
Aprendizaje profundo	Refiere a un subconjunto del aprendizaje automático que utiliza redes neuronales multicapa, generalmente de gran tamaño, con grandes conjuntos de datos, para realizar tareas de predicción. Los principales ejemplos de avances recientes en el ámbito del aprendizaje automático, como los modelos de lenguaje de gran tamaño, en general pertenecen a esta categoría.

Término	Explicación
Aprendizaje supervisado	Describe un subconjunto del aprendizaje automático en que los conjuntos de datos de entrenamiento están etiquetados de modo que el modelo aprenda a asociar datos de entrada con datos de salida específicos. Un ejemplo sería desarrollar un modelo para convertir la escritura a mano en texto, para lo que se entrenaría al modelo con un conjunto de datos de muestras de escritura a mano y sus equivalentes en texto.
Exactitud	Es una medida del porcentaje de datos de entrada que un modelo clasifica correctamente.
Modelos de lenguaje de gran tamaño (LLM)	Son el resultado de los avances recientes del aprendizaje profundo en el campo del procesamiento del lenguaje natural, principalmente debido al desarrollo de la arquitectura de transformadores, que han dado lugar a modelos entrenados en grandes extensiones de texto. Se pueden utilizar los LLM, como ChatGPT, LLaMA y Gemini, para generar, interpretar y clasificar texto.
IA discriminatoria	Describe un subconjunto del aprendizaje automático que utiliza modelos para clasificar o separar datos. Los LLM que se usan para clasificar texto como sentimientos “positivos” o “negativos” son ejemplos de IA discriminatoria.
IA generativa (IAG)	Describe un subconjunto del aprendizaje automático que utiliza modelos para generar contenido, a menudo texto, video o audio. Los LLM que se utilizan como *chatbots* son ejemplos de IA generativa.
Interpretabilidad	Describe la capacidad de las personas para entender cómo toma decisiones un modelo. Por ejemplo, la regresión lineal es un modelo generalmente interpretable, ya que es fácil entender los coeficientes que el modelo aplica a cada factor. En cambio, en una red neuronal multicapa es mucho más difícil interpretar por qué determinados datos de entrada generan ciertos resultados de salida.
Métodos estadísticos tradicionales	Se trata de métodos estadísticos que se utilizan desde hace mucho tiempo, como las regresiones lineales y logísticas. En muchos casos se han utilizado estos métodos para inferir o formalizar la comprensión de datos.

Sobre el autor

Prathm Juneja es doctorando y becario Rhodes en el Oxford Internet Institute de la Universidad de Oxford, donde se dedica principalmente a investigar el papel que la IA y otras tecnologías digitales pueden desempeñar para mejorar el funcionamiento, la accesibilidad y la equidad de las elecciones. El autor también ha analizado la ética relacionada con la IA, las políticas tecnológicas, el aprendizaje automático y el comportamiento electoral. Prathm asesora regularmente a empresas, organizadores, gobiernos y campañas políticas sobre el uso de la IA, las políticas públicas digitales y la política de la tecnología.

Acerca de IDEA Internacional

El Instituto Internacional para la Democracia y la Asistencia Electoral (IDEA Internacional) es una organización intergubernamental con 35 estados miembros, fundada en 1995 con el mandato de apoyar la democracia sostenible en todo el mundo.

QUÉ HACEMOS

Desarrollamos investigaciones favorables a las políticas y análisis relacionados con elecciones, parlamentos, constituciones, digitalización, cambio climático, inclusión y representación política, todo ello bajo el paraguas de los Objetivos de Desarrollo Sostenible de la ONU. Evaluamos el desempeño de las democracias a través de nuestro singular Índices del estado global de la democracia y el Observador de la democracia.

Ofrecemos desarrollo de capacidades y asesoramiento experto a los actores democráticos incluyendo a los gobiernos, los parlamentos, los funcionarios electorales y la sociedad civil. Desarrollamos herramientas y publicamos bases de datos, libros, y guías en varios idiomas sobre temas que van desde la participación electoral hasta las cuotas de género.

Acercamos a los actores estatales y no estatales para establecer diálogos y compartir aprendizajes. Nos hemos consagrado con promover y proteger la democracia mundial.

DÓNDE ACTÚA IDEA INTERNACIONAL

Nuestra sede se encuentra en Estocolmo. Contamos con oficinas regionales y nacionales en África y Asia Occidental, Asia-Pacífico, Europa y América Latina y el Caribe. IDEA Internacional es Observador Permanente de la ONU y está acreditada como institución en la Unión Europea.

NUESTRAS PUBLICACIONES Y BASES DE DATOS

Tenemos un catálogo con más de 1.000 publicaciones y más de 25 bases de datos en nuestro sitio web. La mayoría de nuestras publicaciones se pueden descargar de forma gratuita.

<https://www.idea.int>

IDEA Internacional
Strömsborg
SE-103 34 Estocolmo
SUECIA
+46 8 698 37 00
info@idea.int
www.idea.int

Ahora que la inteligencia artificial (IA) y el papel que esta podría desempeñar en las elecciones se han convertido en un tema que cobra cada vez más importancia, es necesario que los organismos electorales elaboren planes para responder a la IA, así como para utilizarla, en algunos casos, a fin de garantizar elecciones libres, justas y seguras. La IA es un conjunto de tecnologías en rápida evolución que en gran medida carecen de regulación. Además, hasta el momento se ha investigado muy poco su posible impacto en las elecciones.

El objetivo de este informe es brindar apoyo a los organismos electorales y a otros actores interesados a fin de promover una amplia comprensión de las oportunidades, los retos y las implicaciones jurídicas del uso de la IA en las elecciones.

ISBN: 978-91-7671-842-1 (versión en pdf)