Red Mundial
de Justicia Electoral

Panorama Normativo y Judicial del uso de la Inteligencia Artificial en los Procesos Electorales

Versión: octubre 2024

Coordinación general: Consejo del Observatorio de Redes Sociales

Comité de redacción: Secretaría Técnica de la RMJE

Coordinación Académica: Frederico Franco Alvim y Vitor de Andrade Monteiro

Las opiniones expresadas en esta publicación pertenecen a las personas autoras y no necesariamente representan las opiniones de las y los miembros del Consejo Directivo del Observatorio de Redes Sociales, ni del Tribunal Electoral del Poder Judicial de la Federación de México (TEPJF).

ÍNDICE

Prólogo

Los siguientes comentarios surgen de un análisis final de las y los miembros del Consejo Directivo del Observatorio de Redes Sociales, los cuales se sugiere considerar antes de leer este documento.

El análisis normativo y jurídico del uso de la inteligencia artificial (IA) en los procesos electorales llega en un momento oportuno. A medida que un número creciente de elecciones se ve influenciado por la IA, se hace necesario sostener discusiones científicas. Este documento no es un trabajo concluyente, sino un excelente punto de partida para un estudio continuo.

Actualmente, existe una brecha significativa entre las expectativas generadas por la IA y su aplicación real. Debido al rápido avance de esta tecnología, el presente informe se enfoca principalmente en proyecciones pues resulta más útil explorar posibles escenarios futuros ya que los presentes tienden a perder vigencia con rapidez.

La IA en el contexto electoral es un campo amplio y en constante evolución. Por ello, es importante aclarar a las personas lectoras el significado de conceptos clave como la IA general (AGI, por sus siglas en inglés), que busca replicar tareas humanas, y la IA generativa (GenAI, por sus siglas en inglés), que utiliza información existente como base para generar contenido nuevo como imágenes, videos y textos, entre otros. Esta distinción es crucial al debatir la parcialidad de la IA, la legitimidad de sus aplicaciones y la procedencia de los contenidos. Es importante destacar que personas funcionarias, juezas y representantes de la sociedad civil suelen tener dificultades para distinguir entre las distintas aplicaciones de los modelos de IA. Además, estas tecnologías no son excluyentes, ya que una aplicación de GenAI puede ser parte de una AGI.

Futuros trabajos deberían abordar riesgos adicionales asociados al uso de la IA, particularmente las capacidades y precisiones atribuidas a esta tecnología. Esto incluye tecnologías como el reconocimiento biométrico, donde muchos proveedores distorsionan la precisión de sus herramientas, y otras tecnologías, como las de escucha, que presentan problemáticas similares. Los organismos de gestión electoral suelen dedicar demasiado tiempo a amenazas percibidas, como los *deepfakes*, que en realidad no representan una

problemática prioritaria en elecciones recientes. Por otra parte, se destaca la relevancia de señalar la presencia de la IA integrada y las funcionalidades de la realidad aumentada en herramientas cotidianas, dado que estos elementos serán cada vez más frecuentes en la resolución de disputas electorales.

En resumen, este trabajo tiene como objetivo analizar el panorama y los usos de la IA en el mundo en materia electoral, proporcionando un punto de partida para guíar futuras investigaciones y fomentar un entendimiento más profundo de una tecnología en constante evolución.

1. Introducción

Las elecciones operacionalizan un modelo específico de legitimación del poder político, basado en que el ejercicio de las funciones representativas es conferido a agentes que derivan la fuente primaria de su autoridad del consentimiento de la sociedad como un todo (Caretti; De Siervo, 2017). Este consentimiento, a su vez, dialoga directamente con la preservación de un escenario favorable a la materialización de elecciones libres e informadas, de modo que la soberanía popular adquiera realmente una expresión auténtica.

Inicialmente, la protección de la libertad de sufragio y, consecuentemente, la agenda a favor de elecciones democráticas se centraba en el combate a la violencia, al fraude y al abuso, presuponiendo medidas institucionales contra la alteración de procedimientos y documentos oficiales (como actas, papeletas y mapas de escrutinio), así como la eliminación de conductas relacionadas con el abuso de poder económico y político (prácticas clientelistas, caudillistas y similares). Con el tiempo, la preservación de la autonomía ha pasado a incorporar, en relación con la expansión del poder de influencia de los grandes medios de comunicación y las nuevas tecnologías, la necesidad de garantizar la igualdad de oportunidades en el ámbito publicitario, el equilibrio y la pluralidad de opiniones en la cobertura periodística y, más recientemente, la veracidad e integridad del entorno informativo, la seguridad en la gestión de datos, la transparencia en la publicidad informática y la neutralidad político-partidista de las tecnologías disruptivas.

Desde hace algún tiempo, se entiende que la plena libertad de voto no significa la simple ausencia de coacciones directas en forma de sobornos, amenazas o constricciones, y que es necesario preservar otros atributos de la autodeterminación, entre ellos la contención de los procesos de desinformación que distorsionan la comunicación circulante (Alvim, 2024), incluyendo formas de ingeniería social basadas en la explotación de datos personales para aplicar presiones psicométricas y otras formas de manipulación que perjudican la reflexión (Han, 2022), diezman la capacidad analítica (Durand, 2023) y dificultan la adopción de una "actitud paciente y atenta frente al mundo" (Sandel, 2022).

Como observa Lozano (2020), la dispersión de la atención y el colapso de la conciencia conducen a "consecuencias morales" en varios niveles: el exceso de información y el empobrecimiento de la atención desencadenan una "desconfianza epistémica" (Ramonet, 2022) que genera no sólo consecuencias cognitivas, sino también políticas (Lozano, 2020) y conductuales (Klein, 2020), particularmente propicias a la fijación del pensamiento dogmático y a la política de la división. De hecho, la falta de racionalidad disminuye la calidad de los debates colectivos, creando un espacio público receptivo a la

propaganda desinformativa, que se convierte en una característica permanente, tanto dentro como fuera de las campañas oficiales, para debilitar las elecciones (Lissanu; Moraga; Sobol, 2024)[1], profundizar fracturas (Kertysova, 2018), atacar instituciones (Harari, 2024), desestabilizar gobiernos, demonizar opositores, justificar medidas de fuerza (Souza Neto, 2020) y reforzar agendas extremistas (Vlachos, 2022) y campañas de injerencia extranjera (Gillespie, 2018).

En esta coyuntura, la defensa consciente de intereses da paso a comportamientos políticos más orientados hacia estímulos (des)afectivos, lo que conduce a "polarizaciones políticas radicalizadas" (Abranches, 2020) que intensifican la desconfianza, la intransigencia, el extremismo (Slowing-Romero; Scriven, 2024) y el nivel de conflictividad en las contiendas electorales (Fundación Koffi Annan, 2020) y en el propio paisaje social (Nunes; Traumann, 2023).

Esta "era de la irracionalidad deliberada" (Levitin, 2019), por otra parte, transforma las campañas en "guerras cognitivas", haciendo necesaria, además de la agenda de fortalecimiento de la integridad, la adopción de medidas para preservar la normalidad electoral, especialmente en lo que respecta a la recuperación de su vocación civilizada, basada en el antagonismo pacífico como método de sustitución de la hostilidad abierta, la agresión mutua y el conflicto agudo (Alvim; Zilio; Carvalho, 2024). Y es que las nuevas tecnologías en general, y los medios sociales en particular, parecen "poner de manifiesto lo más indeseable de la libertad de expresión: no el debate informado, productivo y razonable sobre asuntos de interés público, sino la desinformación, la agresión" (Barcellos; Terra, 2022) y la "radicalización a gran escala" (Fisher, 2023) en las redes.

Estos dilemas no son precisamente nuevos. En todos los continentes, los órganos de administración electoral, de una forma u otra, conviven con la desinformación, los ataques sistemáticos a la reputación (Alvim, 2021) y fenómenos adyacentes -como el discurso de odio y la intolerancia *en* línea- desde hace casi una década. Sin embargo, la rápida expansión de la inteligencia artificial (IA) tiende a redimensionar el horizonte de problemas, profundizando los desafíos (Bahri et al., 2024) y generando nuevas, robustas e ineludibles necesidades institucionales, teniendo en cuenta que el abuso electoral de la computación inteligente plantea un problema real, no una conjetura hipotética (Sapada; Arif, 2024).

[1] La crisis de confianza ha golpeado duramente la estabilidad de los contenciosos electorales, contribuyendo a la aparición de una verdadera epidemia de resultados impugnados. Según un importante informe publicado recientemente por IDEA Internacional (2024), en los dos últimos años, en el 20% de las elecciones nacionales, al menos un candidato o partido derrotado rechazó públicamente la aceptación de los resultados, y en una proporción idéntica hay decisiones que deben decidir los tribunales.

Así, este estudio aborda las transformaciones provocadas por la progresiva incorporación de soluciones de IA en las campañas electorales, con énfasis en los impactos de la nueva comunicación política sobre la estabilidad democrática y sobre el microsistema de protección de la normalidad e integridad de los procesos electorales. Sus reflexiones parten de la premisa de que identificar claramente los riesgos y comprender plenamente los medios por los que opera la inteligencia artificial en el contexto político son condiciones indispensables para formular estrategias capaces de mitigar sus efectos negativos, con el objetivo de garantizar la autenticidad de las elecciones y el futuro de la democracia (Yu, 2024).

El objetivo de este trabajo será analizar las experiencias regulatorias ya desarrolladas en todo el mundo, así como los enfoques judiciales sobre el uso de la IA en las elecciones. Por último, se presentarán recomendaciones para una mejor adaptación y mejora de las organizaciones electorales ante la nueva era de elecciones algorítmicas.

2. Metodologias y modelo de análisis

La investigación utiliza una combinación de técnicas, implicando, en primer lugar, un estudio descriptivo aplicado a definir la inteligencia artificial, mapear sus usos políticos (positivos y negativos) y los correspondientes impactos en aspectos clave de la gobernanza electoral. Desde esta perspectiva, se perfilará el fenómeno investigado en consonancia con una revisión en profundidad de la literatura disponible, buscando un enfoque multidisciplinaria con aportaciones doctrinales de las ciencias tecnológicas, la Ciencia Política, la Comunicación Social, la Ética de la Tecnología y diversos campos del Derecho (Constitucional, Digital, Internacional y Electoral).

Al mismo tiempo, el examen del *corpus* jurisprudencial se orientará por la metodología de análisis de las decisiones judiciales mediante la técnica exploratoria de observación documental, aplicándose el mismo método a la investigación del campo normativo. En este ámbito, se pretende recoger una muestra relevante de las decisiones judiciales que puedan existir, con el fin de esbozar un primer "estado del arte" (Freitas Filho; Lima, 2010) sobre el objeto definido.

El segmento legislativo, por su parte, será examinado, interpretado y clasificado desde diez perspectivas diferentes, relativas a: i) la amplitud del tratamiento normativo; ii) el rango normativo de las normas; iii) la premisa de la matriz reguladora; iv) la orientación general de las iniciativas; v) el ámbito de aplicación de las normas aprobadas; vi) los

destinatarios de las normas sancionadoras; vii) la naturaleza y el alcance de las sanciones previstas; viii) los estratos de actuación cubiertos; ix) el objeto de protección de las normas que regulan el contenido; y x) el grado de cobertura de los riesgos cartografiados.

Cuadro 1: Dimensiones de análisis del *corpus* normativo

Dimensión del análisis	Categorías previstas
1. Ámbito de aplicación del tratamiento reglamentario	a) intervención sistemática b) intervención microsistemática c) intervención puntual.
2. Rango normativo de las normas	a) normas constitucionales; b) normas comunitarias c) normas jurídicas (actos primarios) d) infralegales (actos secundarios)
3. Premisa de la matriz normativa	a) regulación basada en el riesgo; b) regulación basada en los derechos c) regulación híbrida.
4. Orientación general de la iniciativa	a) marcos reglamentarios permisivos b) marcos normativos prohibitivos c) marcos normativos híbridos.
5. Ámbito de aplicación de las normas aprobadas	a) normas antimonopolio; b) normas de protección de datos c) normas sobre responsabilidad por incumplimiento de órdenes judiciales o por contenidos ilícitos de terceros; d) normas sobre el deber de diligencia.
6. Destinatarios de las normas sancionadoras	a) candidatos y organizaciones de partidos; b) plataformas de medios sociales c) desarrolladores y proveedores de soluciones de IA d) productores de contenidos e influenciadores digitales e) medios de prensa f) personas politizadas y usuarios en general.
7. Naturaleza de las sanciones previstas	a) retirada de contenidos; b) imposición de multas c) suspensión o prohibición de perfiles, cuentas o canales d) desconexión o interrupción del suministro de servicios e) cancelación del registro de candidaturas o mandatos políticos f) declaración de inelegibilidad (inhabilitación) g) anulación de elecciones.

8. Estratos de la acción legislativa	a) *la necesidad de autorización para prestar servicios de carácter electoral* b) el *modelo de negocio* (cuando se aprueben normas que condicionen la comercialización de productos o servicios, o que estipulen parámetros aplicables a la remuneración de los productores de contenidos); c) *la programación algorítmica* (cuando se fijen pautas u orientaciones aplicables a la calibración de algoritmos de clasificación, selección y recomendación); d) *responsabilidad social* (cuando se establecen obligaciones para compensar o restaurar el entorno informativo ante casos de desinformación); e) *control de comportamientos* (cuando se establece la prohibición de acciones inauténticas, como el uso de perfiles falsos, agentes robotizados o herramientas de disparo masivo); y e) *control de contenidos*
9. Bienes jurídicos protegidos	a) *la libertad de ejercicio del sufragio*; b) la *igualdad de oportunidades de los competidores políticos*; c) el *honor o la imagen de candidatos y partidos*; d) la *intimidad de los internautas*; e) *la dignidad y seguridad de las personas pertenecientes a grupos vulnerables o minoritarios*; f) *el honor, la imagen o la confianza en las instituciones de garantía* (tribunales u órganos de administración electoral); g) *el carácter pacífico de las elecciones, la estabilidad democrática y la paz social*
10. Grado de cobertura de los riesgos mapeados	(a) *normas contra la desinformación y el comportamiento no auténtico*; (b) *normas dirigidas a la prevención de conflictos*; (c) *normas contra la manipulación de los flujos de información a través de algoritmos*; (d) *normas contra el acoso, la discriminación y la violencia política*; (e) *normas contra el uso abusivo o irregular de datos personales*; y (f) *normas para preservar la eficacia del sistema de rendición de cuentas basado en controles oficiales*.

Fuente: elaboración propia.

En términos de **amplitud** o alcance, los marcos disciplinarios se clasificarán como: a) *sistemáticos* (cuando dan un tratamiento integral al tema de la inteligencia artificial, a raíz de leyes que tratan aspectos más amplios que el proceso electoral); b) *microsistemáticos* (cuando se moldean en reformas electorales que tratan la IA de manera integral); o c) *puntuales* (cuando las leyes electorales tratan aspectos aislados de la inteligencia artificial de manera específica, concisa y escasa).

Desde la perspectiva **del alcance de la intervención jurídica**, las normas se clasificarán según el origen y la naturaleza del proceso normativo. Así, las disposiciones se clasificarán en: a) *constitucionales* (cuando actualicen o modifiquen disposiciones de las constituciones nacionales); b) *comunitarias* (cuando procedan de actos aprobados por parlamentos supranacionales); c) *legales* (cuando sean aprobadas por parlamentos nacionales y tengan el *rango de* actos normativos primarios); y d) *infralegales* (cuando deriven directamente de decretos del poder ejecutivo o de instrucciones dictadas por tribunales u órganos de la administración electoral legalmente habilitados para ello).

La premisa de la matriz reguladora implica un análisis panorámico del espíritu rector de las soluciones normativas. A través de esta lente, las muestras se clasifican en: a) *modelos basados en el riesgo* (cuando se limitan a imponer deberes y prever sanciones); b) *modelos basados en la protección de derechos* (cuando establecen principalmente garantías para los usuarios, las partes interesadas y/o la población en general); o c) *modelos híbridos* (cuando incluyen prescripciones que se encuadran en ambas categorías).

Atendiendo a su **orientación general**, los marcos reguladores se clasificarán en las siguientes categorías: a) *marcos permisivos* (cuando se identifican exclusivamente normas que aclaran las hipótesis en las que está permitido el uso de la IA); b) *marcos* prohibitivos (cuando se identifican exclusivamente normas que señalan las hipótesis en las que está prohibido el uso de la IA); o c) *marcos híbridos* (cuando se identifica la confluencia de normas permitidas y prohibitivas).

En cuanto **al alcance de las normas aprobadas**, se trata de conocer, a efectos de destacar, la opción de promulgar: a) normas *antimonopolio* (centradas en restricciones o regulaciones de la competencia); b) *normas sobre protección de datos*; c) *normas destinadas a exigir responsabilidades a los actores políticos*; d) *normas destinadas a exigir responsabilidades a las grandes tecnológicas* (por ejemplo, en casos de *incumplimiento de órdenes judiciales* o de contenidos ilegales publicados por terceros); e) *normas que establezcan un deber de diligencia impuesto a los* desarrolladores *o proveedores de herramientas de IA y/o plataformas de medios sociales*, en casos de incumplimiento de órdenes judiciales o contenidos ilegales publicados por terceros); e) *normas que establezcan un deber de diligencia* impuesto a los desarrolladores o proveedores de herramientas de IA y/o plataformas de medios sociales.

El análisis de **los destinatarios de las normas sancionadoras** orienta la investigación hacia la detección y correspondiente focalización de las normas que prevén respuestas jurídicas negativas contra: (a) *candidatos y entidades partidistas* (partidos políticos, federaciones, coaliciones o alianzas de cualquier tipo); (b) *plataformas de medios*

sociales (redes sociales, *microblogs*, buscadores, apps de mensajería privada, portales de alojamiento de vídeos); (c) *desarrolladores y proveedores de inteligencia artificial*; (d) *productores de contenidos e influencers digitales*; (e) *medios de prensa* (en soporte físico, analógico o digital); y (f) personas politizadas y usuarios en general (activistas, simpatizantes y particulares de a pie).

En cuanto a la **naturaleza de las sanciones** que pueden preverse, la encuesta considerará la presencia de normas que legitimen la elaboración de órdenes administrativas o judiciales restrictivas, destinadas a: a) *retirar contenidos*; b) *imponer multas pecuniarias*; c) *suspender o prohibir perfiles, grupos o canales en medios sociales*; d) *desconectar o interrumpir el suministro de servicios de aplicaciones de Internet*; e) *revocar inscripciones de candidaturas o mandatos políticos*; f) *declarar la inelegibilidad o la inhabilitación*; y g) *anular elecciones*.

En cuanto a los **estratos de la acción legislativa**, concretamente en lo que se refiere al funcionamiento de las plataformas de medios sociales, se estudiarán las normas que afecten a a) *la necesidad de autorización para prestar servicios de carácter electoral* (cuando se prevea algún tipo de registro o medida obligatoria para garantizar el funcionamiento legal de las plataformas durante el periodo electoral); b) el *modelo de negocio* (cuando se aprueben normas que condicionen la comercialización de productos o servicios, o que estipulen parámetros aplicables a la remuneración de los productores de contenidos); c) *la programación algorítmica* (cuando se fijen pautas u orientaciones aplicables a la calibración de algoritmos de clasificación, selección y recomendación); d) *responsabilidad social* (cuando se establecen obligaciones para compensar o restaurar el entorno informativo ante casos de desinformación); e) *control de comportamientos* (cuando se establece la prohibición de acciones inauténticas, como el uso de perfiles falsos, agentes robotizados o herramientas de disparo masivo); y e) *control de contenidos* (cuando se encuentran dispositivos para regular el discurso o crear hipótesis de abuso lingüístico).

En cuanto a los **bienes jurídicos protegidos por las normas de limitación de contenidos**, las disposiciones localizadas se clasificarán en función de si pretenden proteger: a) *la libertad de ejercicio del sufragio*; b) la *igualdad de oportunidades de los competidores políticos*; c) el *honor o la imagen de candidatos y partidos*; d) la *intimidad de los internautas*; e) *la dignidad y seguridad de las personas pertenecientes a grupos vulnerables o minoritarios*; f) *el honor, la imagen o la confianza en las instituciones de garantía* (tribunales u órganos de administración electoral); o g) *el carácter pacífico de las elecciones, la estabilidad democrática y la paz social*. Dadas las evidentes peculiaridades, las normas que aquí se analizan pueden clasificarse de más de una manera.

Por último, en cuanto al **grado de cobertura de los riesgos mapeados**, se observará la presencia de dispositivos capaces de contrarrestar las principales amenazas sistémicas derivadas del uso malicioso de la IA en el contexto electoral, en particular por la existencia de: (a) *normas contra la desinformación y el comportamiento no auténtico*; (b) *normas dirigidas a la prevención de conflictos*; (c) *normas contra la manipulación de los flujos de información a través de algoritmos*; (d) *normas contra el acoso, la discriminación y la violencia política*; (e) *normas contra el uso abusivo o irregular de datos personales*; y (f) *normas para preservar la eficacia del sistema de rendición de cuentas basado en controles oficiales*.

Finalmente, la información recabada será analizada desde una perspectiva descriptivo-prescriptiva (Sapada; Arif, 2024), con el fin de elaborar un catálogo de recomendaciones fundamentadas, capaces de orientar las acciones institucionales encaminadas a la defensa institucional de la integridad electoral frente a los riesgos derivados del uso indebido de las nuevas tecnologías informáticas.

3. La inteligencia artificial como tecnología fundacional y el nuevo orden de la comunicación política

La inteligencia artificial se manifiesta en sistemas o dispositivos tecnológicos capaces de reproducir las capacidades cognitivas de los seres humanos, cumpliendo tareas, proponiendo alternativas o resolviendo problemas de diversa complejidad, mediante actuaciones electrónicas basadas en el aprendizaje, el razonamiento, el cálculo, la creatividad o la memorización (Degli-Esposti, 2023). Cuando se trata de IA, por lo tanto, estamos ante dispositivos informáticos "activos", es decir, herramientas tecnológicas que "aprenden, crean por sí mismas y se vuelven intuitivas", siendo capaces de "predecir situaciones futuras sin intervención humana y sin tener que empezar de cero con cada nueva situación" (Gabriel, 2022).

En términos generales, las soluciones inteligentes reducen costos, simplifican, agilizan, mejoran y, en algunos casos, automatizan actividades y procesos de trabajo básicos, lo cual hace que se integren a innumerables frentes gubernamentales, científicos e industriales, así como asimilándose paulatinamente a las prácticas políticas y sociales, con importantes repercusiones que afectan, entre otros ámbitos, a la densidad democrática[2]

[2] El grado de materialización de los presupuestos democráticos

(Innerarity, 2024; Kreps; Kriner, 2023) y la eficacia de las constituciones nacionales (Balaguer Callejón, 2023), particularmente en lo que se refiere a la defensa de las libertades públicas y otros derechos fundamentales, como la intimidad, la privacidad, la protección de datos, la igualdad, el voto libre e informado (Rubio Núñez; Alvim; Monteiro, 2024), el sufragio secreto (Mainz; Sønderholm; Uhrenfeldt, 2022) y la concurrencia a cargos representativos en condiciones de equidad (Sánchez Muñoz, 2020).

Las aplicaciones de IA reorganizan el espacio público, promueven la reconfiguración de las relaciones de poder y, por tanto, se consideran más "medios sociotécnicos" que simples instrumentos tecnológicos (Pérez de Lama; Sánchez-Laulhé, 2020). Es más, la inteligencia artificial puede considerarse una "tecnología fundacional", ya que tiene un potencial de transformación sin precedentes, que promete "remodelar nuestro mundo de maneras que son a la vez fascinantes y aterradoras" (Suleyman; Bhaskar, 2024), dada su naturaleza maleable y dual.

Las transformaciones radicales, por cierto, ya se están acelerando en el entorno de la información, dando lugar a la aparición de un nuevo panorama histórico: la era de las "elecciones algorítmicas" (Bender, 2022) o era de las “*smart elections”* (Hammar, 2024), vista como una etapa irreversible, emocionante y desafiante en la competencia por el voto ciudadano.

3.1 Inteligencia artificial en favor de la democracia

En cualquier caso, hay que destacar que la inteligencia artificial, a pesar de desvelar un preocupante conjunto de problemas potenciales, trae consigo un abanico igualmente amplio de alternativas positivas (Kertsysova, 2018; Stevenson, 2024), y puede ser utilizada dentro del universo electoral con fines lícitos y socialmente deseables, incluso como un activo estratégico indispensable para que los organismos electorales corrijan injusticias históricas (Bender, 2022), enfrenten amenazas presentes e intensifiquen la integridad en el futuro (Rubio Núñez; Alvim; Monteiro, 2024). Bajo esta perspectiva, en lugar de ser entendida exclusivamente como una fuente inagotable de problemas, la computación inteligente debe ser vista como un fenómeno emergente ambivalente, ciertamente cargado de desafíos, pero igualmente rico en ofrecer oportunidades significativas para las instituciones dedicadas a proteger las elecciones (Hammar, 2024; Juneja, 2024; Sapada; Arif, 2024; Suárez, 2024).

De este modo, la IA simplifica y mejora las rutinas de trabajo, asumiendo tareas repetitivas, eliminando errores, descubriendo nuevos métodos y reduciendo los costos económicos y *los plazos de* realización. Además, procesa datos estructurados y no estructurados para realizar estudios de coyuntura, cálculos situacionales, evaluaciones de respuestas sentimentales y patrones de voto, así como para desarrollar análisis predictivos que ahora son indispensables para una comunicación eficaz. Además, el desarrollo del lenguaje natural permite automatizar las interacciones con el público y reducir drásticamente los costos intelectuales normalmente necesarios para diseñar notas informativas y persuasivas. Dentro de este espectro, la inteligencia artificial tiene la capacidad de turbo alimentar las campañas políticas, ofreciendo ventajas tácticas en términos de optimización del alcance y contenido de los mensajes, recopilación de información, anticipación de resultados, análisis estadístico, segmentación del electorado y detección de tendencias de comportamiento, entre otras posibilidades que se renuevan día a día en una espiral que parece infinita (Rubio Núñez; Alvim; Monteiro, 2024).

En términos esquemáticos, la IA da lugar a un "cambio de paradigma" (Safiullah; Parveen, 2021) en las contiendas electorales, como efecto de un sinfín de alternativas sociotécnicas que pueden afectar, por ejemplo, a campos como: a) la planificación estratégica; b) las actividades de gestión; c) la generación y reenvío de respuestas instantáneas; d) la adopción de modelos predictivos; e) la mejora de los procesos de recogida, categorización y análisis de datos; f) la mejora de la comunicación con los votantes; g) el aumento y la medición de la eficiencia; h) la apertura de canales de comunicación a través de *chatbots* y asistentes virtuales; i) optimización de tareas logísticas; j) el conocimiento del votante, la segmentación de los votantes y el envío de mensajes personalizados; k) la creación de publicidad; l) el seguimiento de temas y debates en tiempo real; m) análisis de discursos y sentimientos; n) investigación de la oposición; o) contraste de campañas y ataque a los oponentes; p) redacción de discursos; q) actividades de reacción pública; r) seguimiento de costos y gastos; s) predicción de resultados; t) recopilación de información clave para programar visitas a domicilio; u) construcción, legitimación y pulido de la imagen pública; y v) optimización de la recaudación de fondos e identificación de donantes (Hammar, 2024; Okoye, 2024; Tomić; Damnjanović; Tomić, 2023; Valdez Zepeda; Aréchiga; Daza Marco, 2024).

En la misma línea, en el ámbito institucional, la inteligencia artificial es capaz de organizar y depurar el censo electoral (Chennupati, 2024) y mejorar el esquema de supervisión electoral (Stevenson, 2024), tanto en lo que respecta al refuerzo de la seguridad y la prevención de la violencia en los colegios electorales (Deepak; Simoes; MacCarthaigh,

2023)[3] como, especialmente, en el ámbito de la lucha contra el discurso nocivo y la desinformación en línea (Kertysova, 2018), así como optimizar la verificación de firmas en actas (por ejemplo, voto por correo) y peticiones públicas (por ejemplo, para respaldar a candidatos independientes o formar partidos públicos), y peticiones públicas (por ejemplo, para respaldar a candidatos independientes o formar nuevos partidos políticos), la forma en que se asignan los distritos (Bender, 2022) y los mecanismos de control y certificación de las actividades financieras de candidatos y partidos, así como la agilización de la resolución de procedimientos administrativos y causas judiciales, proporcionando mayor seguridad, transparencia y eficiencia en los actos de gestión y la adjudicación de justicia.

Otras posibles aplicaciones por parte de los organismos de administración electoral, en una lista no exhaustiva, incluyen técnicas de modelización estadística para previsiones presupuestarias y decisiones de asignación de recursos, estudios para la racionalización de la distribución (Okoye, 2024) y el posicionamiento estratégico de los colegios electorales (o centros de cómputo) (Juneja, 2024), seguimiento de la programación de emisoras de radio y televisión en cuanto al cumplimiento del tiempo asignado a la publicidad electoral, supervisión del cumplimento de jornadas de reflexión o leyes de silencio (Bozkurt, 2024), detección temprana de averías o fallos en las máquinas de votación y recuento de votos mediante tecnologías de vídeo (Deepak; Simoes; MacCarthaigh, 2023), así como la supervisión, organización y difusión del origen y la suma de los recursos financieros recaudados o gastados en actividades de campaña, incluidas las inversiones en anuncios u otras formas de publicidad digital.

La IA también puede ser útil en las prácticas de auditoría postelectoral, por ejemplo, para detectar incidentes de fraude. De este modo, los modelos desarrollados con antelación pueden proporcionar comparaciones contrastadas con los resultados electorales reales. Además, las aplicaciones del aprendizaje automático y las estadísticas tradicionales pueden señalar colegios electorales que muestren diferencias significativas en comparación con otros colegios electorales, sirviendo de punto de partida para futuras investigaciones policiales o forenses (Juneja, 2024).

En la misma línea, las aplicaciones basadas en grandes modelos de lenguaje (LLM) y, sobre todo, en IA generativa son especialmente útiles para potenciar *el prebunking*

[3] En este sentido, los expertos comentan que la IA puede aplicarse para justificar la detención preventiva de posibles delincuentes, así como para identificar colegios electorales que, por aspectos clave como un historial de delincuencia o altercados, requieran protección policial adicional. Además, las tecnologías inteligentes pueden reconocer grupos vulnerables de votantes (como minorías oprimidas) cuya protección es necesaria para garantizar la integridad del proceso. Por último, los sistemas de cámaras basados en IA permiten una vigilancia automatizada generalizada y escalable que resulta más eficaz que la vigilancia humana para detectar fraudes o intentos de fraude en tiempo real (Deepak; Simoes; MacCarthaigh, 2023).

*(*imunizar*)* y el *debunking* (desmentir) de noticias falsas, reforzar los enfoques de fact-checking (incluidos *los chatbots*), ahorrar tiempo y optimizar la comunicación de crisis[4]. Otras alternativas pasan por el desarrollo de soluciones inteligentes para detectar comportamientos no auténticos derivados de herramientas de *difusión* y campañas de *spam*, así como *software de* "*bot-spotting*" o *"bot-labelling"* (marcación de bots) utilizado para marcar y eliminar cuentas falsas operadas por *trolls* o robots (Kertysova, 2018). La inteligencia artificial, en la misma línea, puede aplicarse para detectar el uso encubierto de la propia IA en la producción de contenidos de comunicación y la manipulación de los medios digitales en general, por ejemplo, con el apoyo de herramientas como Deep Media, InVID y FakeCatcher (Soon; Quek, 2024). Puede, además, sostener proyectos multiniveles de educación ciudadana, incluso bajo una perspectiva de inclusión (Arnold, 2023), por ejemplo, con recursos de tecnología asistencial.

La implementación de sistemas inteligentes "capaces de analizar patrones sutiles e inconsistencias en vídeos y audios puede proporcionar una capa crucial de protección contra la propagación de la desinformación", además podemos considerar el uso de tecnologías *Blockchain* y *Watermarking* con la implementación de técnicas de autenticación digital para verificar la integridad y el origen de los contenidos audiovisuales" (Tavares, 2024), medidas más que necesarias en la era de las falsedades de segunda generación. Por último, es evidente que la IA puede contribuir de forma sólida a la seguridad de los sistemas electorales, detectando posibles ciber amenazas y ayudando a eliminar las injerencias externas en el proceso electoral (Yazbek, 2024).

Cabe señalar, como precaución, que algunas de estas posibilidades, aunque válidas y prometedoras, no están exentas de contingencias, que deben ser debidamente cartografiadas y sopesadas, a raíz de los mecanismos internos de gobernanza y gestión de riesgos adoptados por los organismos electorales. El análisis de los pros y los contras ya forma parte de las preocupaciones académicas, como ilustra un cuadro extraído de una investigación realizada por investigadores de la Universidad de Belfast:

Cuadro 2: Posibilidades, riesgos potenciales y vías para el uso de la IA en aspectos claves:

Vía	**Uso de la IA**	**Riesgos**	**Caminos**
Gestión de la lista de votantes	Abordajes por enfoques heurísticos Vinculación de registros	Cuestiones de equilibrio entre acceso e integridad	IA centrada en el acceso

[4]La IA puede ser utilizada por los organismos electorales en acciones más triviales, como la traducción inmediata de reuniones, clases o conferencias a un idioma extranjero, facilitando el intercambio de experiencias y conocimientos entre organizaciones aliadas, entre otras muchas aplicaciones posibles.

	Detección de valores atípicos	Sesgos de IA Exceso de generalización de IA	Explicaciones razonables Control local
Ubicación de cabinas electorales	Determinación de ubicación de los buzones Ubicación de las instalaciones Agrupación	Ética organizacional Volatilidad y costos de búsqueda Manipulación partidista	Resultados plurales Auditoría de la IA Votantes desfavorecidos
Predicción de cabinas problemáticas	Vigilancia predictiva Diseño de series históricas	Racismo sistémico Brutalidad agravada Bucles de retroalimentación	Transparencia Rigor estadístico IA justa
Autenticación de los votantes	Reconocimiento facial Biometría	Sesgos de raza o género Sesgos desconocidos Participación Vigilancia y otros	Alternativas Auditoría de sesgos Diseño para casos extremos
Monitoreo por videos	Recuento de votos por vídeo Detección de eventos Re identificación de personas	Integridad Electoral Comunidades marginalizadas Debilitamiento de otros controles	Monitoreo superficial Datos abiertos

Fuente: Deepak; Simoes; MacCarthaigh, 2023 (traducción libre)

A partir de encuestas realizadas por investigadores de varios países, hemos elaborado un catálogo no exhaustivo de soluciones inteligentes ya aplicadas por gobiernos y organismos de administración electoral en varios países del mundo:

- **Argentina**: en junio de este año, la provincia de Corrientes llevó a cabo un proyecto piloto de inteligencia artificial con la lectura de actas mediante redes neuronales secuenciadas (tecnología *de transformadores*) (Suárez, 2024), que resultó exitoso para optimizar y agilizar el proceso de transmisión y recuento de votos.
- **Brasil (a nivel nacional):** el país lleva más de una década utilizando un sistema de reconocimiento facial basado en IA. Esta técnica permite la identificación biométrica en el proceso de habilitación para votar, y también sirve para prevenir el fraude en casos de identidades duplicadas, múltiples o usurpadas en el censo electoral. En la misma línea, se ha implementado el uso de la voz sintetizada por IA para ayudar a las personas con discapacidad visual a votar en las urnas electrónicas, que se utilizará a partir de las elecciones municipales de 2024. El Tribunal Superior Electoral también creó un *chatbot* para servicios al votante en colaboración con WhatsApp, que también se utilizó para desmentir rumores y narrativas de desinformación. Al incluir una función *de inclusión voluntaria*, el chatbot envió alertas proactivas sobre temas importantes con consentimiento. Con más de 6,2 millones de usuarios activos y unos 20 millones de mensajes intercambiados, el chatbot se ha convertido en uno de los mayores de la plataforma en todo el mundo. Además, el TSE, a través de asociaciones estratégicas, cuenta con el apoyo de observatorios de redes y empresas que supervisan los datos abiertos de las redes sociales, proporcionando periódicamente información e informes de análisis sobre la circulación de las principales narrativas de desinformación.
- **Brasil (nivel subnacional):** en el país, algunos tribunales electorales regionales (TRE) han desarrollado soluciones de IA para diversos fines. El sistema *Janus* -desarrollado por el TRE de Bahía y adoptado posteriormente por muchos otros tribunales del país- es una solución de automatización procesal capaz de aumentar la productividad y la eficacia en la prestación

de justicia, agilizando la evaluación de casos de baja complejidad, por ejemplo, en materia de registro de candidaturas y rendición de cuentas de campañas electorales. Además, el tribunal bahiano ofrece a los estudiantes y al público interesado una *visita* inmersiva a través de una experiencia basada en la realidad virtual (incluyendo la posibilidad de utilizar gafas 3D). La TRE de Pernambuco, en otro frente, ha desarrollado un robot para monitorear posts, evaluar contenidos y respuestas con el fin de vigilar el panorama de la desinformación en la red social X durante las elecciones de 2022[5]. Otro proyecto de este tribunal incluyó una herramienta que utiliza IA y robótica para facilitar el proceso de auditoría del funcionamiento de las urnas electrónicas, con vistas a aumentar la confianza de los ciudadanos. Con miras a las elecciones municipales de 2024, la TRE de Goiás lanzó *GuaIA*, una herramienta de análisis de publicaciones en *sitios web* y medios de comunicación, así como de clips de audio y vídeo que contengan noticias distorsionadas o engañosas sobre el proceso electoral. Desde 2022, la TRE de Paraíba aplica la IA a un Sistema de Atención al Votante a Distancia y, a mediados de este año, lanzó un sistema inteligente pionero (*uIAra*), que calcula la probabilidad de que los medios de audio sean *deepfakes*. También en 2024, el TRE de Maranhão lanzó un asistente virtual que utiliza inteligencia artificial para generar ementas (resúmenes de sentencias) para las decisiones judiciales colegiadas dictadas por el tribunal.

- **Canadá**: Los organismos de administración electoral han estado explorando aplicaciones de IA para mejorar la accesibilidad electoral, incluido el desarrollo de *chatbots* para proporcionar información inclusiva a todos los votantes (Yazbek, 2024).
- **Colombia**: la Registraduría Nacional del Estado Civil utiliza herramientas inteligentes en los procesos electorales y de identificación de votantes. Además, se está desarrollando un modelo enfocado en la logística preelectoral capaz de proveer alertas tempranas para que los funcionarios identifiquen circunstancias que merezcan la atención durante todas las etapas organizacionales (Penagos Ramírez, 2024).
- **Corea del Sur:** en las elecciones parlamentarias de 2020, se utilizó un modelo de IA para contar los votos. La tecnología consiguió reducir el tiempo de recuento y mitigar errores humanos examinando los votos adecuadamente mediante técnicas de aprendizaje automático. Esta integración mejoró sustancialmente la eficacia general del proceso electoral (Chennupati, 2024).
- **Estados Unidos:** para hacer el voto más manejable y accesible, el país ha estado investigando el uso de la IA en los sistemas de sufragio. Virginia Occidental es un buen ejemplo: en 2018, el estado puso en marcha un programa de prueba para permitir a los miembros del servicio exterior votar a través de *Voatz*, un *software de* votación móvil. Para garantizar que los votos sean seguros y legítimos, la app emplea algoritmos de IA y tecnología *blockchain*, utilizando datos biométricos y tecnología de reconocimiento facial para proporcionar una identificación precisa de cada votante (Chennupati, 2024). Además, en regiones como Kansas y el Distrito de Columbia, los algoritmos de comprobación cruzada han respaldado programas experimentales de depuración de registros de votantes diseñados para eliminar los casos de votantes registrados indebidamente en dos o más estados de la Unión. Es más, al menos 29 condados de ocho estados diferentes han utilizado programas de verificación de firmas, sobre todo para validar o invalidar votos por correo (Bender, 2022; Juneja, 2024).
- **Estonia:** el país lleva utilizando la IA en los sistemas de votación desde 2005, lo que refuerza su reputación de vanguardia en proyectos de administración electrónica. Un ejemplo es la implantación del sistema *i-voting*, que permite a cualquiera votar en línea de forma segura. En este contexto, los algoritmos de inteligencia artificial desempeñan un papel crucial para

[5] Entre septiembre de 2022 y febrero de 2023, la herramienta AletheIA identificó en Twitter más de 1,9 millones de mensajes desinformativos contra las elecciones brasileñas. Combinando IA y técnicas avanzadas de análisis de datos, el modelo recopila datos abiertos de redes sociales basados en *hashtags* y palabras clave, procesando los textos para eliminar información irrelevante. También clasifica los textos, agrupándolos por sentimientos (positivos o negativos) para ayudar a identificar la desinformación. El sistema también es capaz de enviar automáticamente información oficial a los editores, con explicaciones válidas de los temas previamente categorizados como inapropiados.

garantizar la honestidad del proceso de votación (Chennupati, 2024; Deepak; Simoes; MacCarthaigh, 2023).

- **India**: El Gobierno indio ha estado explorando la IA para mejorar la seguridad electoral, incluida la detección de noticias falsas y la identificación de actividades digitales sospechosas durante el periodo electoral (Yazbek, 2024). Paralelamente, se han probado sistemas de reconocimiento facial de votantes en algunos contextos desde las elecciones municipales de Telangana en 2020. Además, en las elecciones estatales de Bahir en 2021, las autoridades probaron la tecnología de análisis de vídeo para comprobar la exactitud de los votos contados manualmente (Deepak; Simoes; MacCarthaigh, 2023).
- **Indonesia**: impulsado por IA, el Sistema de Información de la Lista de Votantes (*Sidalih*) lleva funcionando desde 2014 para ayudar a la Comisión Electoral General (KPU) a construir bases de votantes íntegros, aumentando la fiabilidad de la consulta popular (Akbar et al., 2021).
- **Libia**: Con el apoyo del Programa de las Naciones Unidas para el Desarrollo (PNUD), la Alta Comisión Electoral Nacional (HNEC) celebró un taller de formación sobre el seguimiento de la violencia en línea contra las mujeres en las elecciones, utilizando herramientas de IA para recopilar datos cuantificables que permitan supervisar y comprender las causas del acoso y la violencia de género digital, con el fin de orientar la búsqueda de soluciones (PNUD, 2022).
- **México:** el Instituto Nacional Electoral (INE) ha desarrollado una herramienta de reconocimiento de texto, que se utilizará a partir de 2024 para la lectura de actas y el recuento de votos con el fin de agilizar la publicación de los resultados preliminares de los procesos electorales (Riquelme, 2023). Al mismo tiempo, el Tribunal Electoral del Poder Judicial de la Federación (TEPJF) está desarrollando un servicio cívico de IA para ayudar a candidatos, partidos políticos y ciudadanos en general a encontrar la mejor vía (administrativa o judicial) para hacer valer sus derechos ante el sistema de justicia electoral (López Ponce, 2024).
- **Nigeria:** La Comisión Electoral Nacional Independiente (INEC) ha puesto en marcha un proyecto piloto para la introducción gradual de la IA en sus operaciones. El *Dispositivo de Inscripción de Votantes de la INEC* (IVED) y el *Sistema de Acreditación Bimodal* (BVAS) mejoran la calidad de la captura de datos en el registro de votantes mediante la aplicación de una tecnología bimodal que reúne huellas dactilares y faciales, en sustitución del modelo inicial centrado exclusivamente en las huellas dactilares. Dentro de la Comisión, el Sistema de Identificación Biométrica Automatizada también utiliza elementos de IA en sus operaciones (Okoye, 2024).
- **Kenia**: a partir de 2017, se implantó un sistema inteligente de identificación biométrica que usa la visión computacional y el escaneo de huellas dactilares para verificar la identidad de los votantes y evitar el fraude electoral (Carter Center, 2022; Yazbek, 2024)[6]. Del mismo modo, con apoyo de la International Foundation for Electoral Systems (IFES), la Comisión Electoral Independiente de Fronteras (IEBC) implementó una herramienta inteligente personalizada que proporcionó una plataforma para detectar, registrar y analizar el discurso de odio en Twitter. A lo largo del ciclo electoral la herramienta permitió a la comisión gestionar mejor las incoherencias fácticas, identificar posibles riesgos para la seguridad y formar a su personal en la supervisión de los medios de comunicación en el Centro Nacional de Recuento (Kolb, 2022).
- **Suiza:** el país también está a la vanguardia de la tecnología, experimentando con nuevas técnicas de votación basadas en *blockchain* e inteligencia artificial. En 2018, la ciudad de Zug puso a prueba un sistema *blockchain* en las elecciones municipales, permitiendo votar a través de dispositivos móviles. Los algoritmos de IA aumentarán la precisión de la identificación de los votantes y reducirán la posibilidad de fraude, mientras que la tecnología

[6] A lo largo de la implementación de ese sistema se descubrió que aproximadamente 1,2 millones de votantes fallecidos todavía seguían figurando en el padrón Electoral (Mosero, 2022), abriendo margen para fraudes en la votación.

blockchain ha permitido un proceso de votación transparente, seguro e inmutable (Chennupati, 2024).

Las nuevas tecnologías también pueden reforzar las funciones de participación y vigilancia que desempeñan los ciudadanos y la sociedad civil[7], por ejemplo, facilitando la organización de intereses colectivos (a través de manifiestos, peticiones y otras formas de demanda), mejorando la accesibilidad del voto (Juneja, 2024) [8] y de los elementos de comunicación, organizando el exceso de información de actualidad, por ejemplo[9]a través de apps que sistematizan y comparan el historial judicial, las plataformas políticas y las fuentes de financiación de los distintos candidatos [10] [11] , y creando herramientas de detección y monitorización de comportamientos inauténticos y de circulación de discursos de odio[12] y desinformación digital en la red, a través de herramientas de escucha social que señalan o incluso anticipan casos de repercusión viral (Kertysova, 2018).

También pueden permitir la producción automatizada de historias periodísticas de interés público, con el objetivo de suplir el déficit de información de las personas que viven en regiones remotas afectadas por el vacío informativo o desierto de noticias (Aramburú Moncada; López Redondo; López Hidalgo, 2023), así como facilitar, a través de aplicaciones de "gamificación" (con herramientas *de cuestionario*) la comparación entre los valores honrados por los votantes y las plataformas de las alternativas en disputa (Machado; Portella, 2024)[13]. Además, la inteligencia artificial permite comprobar de forma

[7] El mismo razonamiento se aplica a los órganos auxiliares de la justicia, como el Ministerio Público Electoral en Brasil. En esta línea, el Ministerio Público de Río de Janeiro en 2024 utilizó la IA para agilizar el proceso de evaluación y eventual impugnación de candidaturas irregulares.

[8] En Israel, OrCam Technologies ha desarrollado el dispositivo *MyEye 2.0*, que aumenta la autonomía de las personas con discapacidad visual. El dispositivo se ha utilizado en el país para que los votantes de este segmento puedan depositar su voto sin ningún tipo de ayuda (Suárez, 2024).

[9] En Suiza, el proyecto Alliance F ha desarrollado un algoritmo llamado *Bot Dog*, responsable de la detección proactiva y automatizada de mensajes que incitan al odio (Suárez, 2024).

[10] "La IA ha contribuido sustancialmente a la accesibilidad electoral mediante la creación de procedimientos de votación alternativos que se adaptan a las necesidades de las personas con discapacidad o problemas de movilidad. Las personas pueden utilizar interfaces accesibles, como lectores de pantalla o comandos de voz, para votar a distancia a través de sistemas de votación electrónica impulsados por inteligencia artificial, lo que permite a las personas votar desde la comodidad de sus hogares. Además de eliminar los obstáculos físicos para votar, estas soluciones garantizan la privacidad y seguridad de los votantes con deficiencias visuales u otras discapacidades. Las interfaces de voz potenciadas por IA han surgido como otra herramienta transformadora para mejorar la accesibilidad en los procesos electorales. Estas interfaces permiten a los votantes con discapacidades motoras o del habla interactuar con los sistemas de votación utilizando comandos de lenguaje natural o instrucciones de audio, facilitando una participación independiente y digna en el proceso electoral. Al eliminar las barreras lingüísticas y de alfabetización, las interfaces vocales permiten a las personas con capacidades diversas ejercer su derecho al voto sin asistencia ni discriminación". (Stevenson, 2024).

[11] La aplicación "Voto Legal", desarrollada por el Movimiento de Combate a la Corrupción Electoral (MCCE) y la iniciativa App Cívico en Brasil, es un buen ejemplo. Con el objetivo de promover unas elecciones más justas y transparentes, la solución utilizaba registros *blockchain* y una interfaz con un lenguaje claro sobre las propuestas políticas, con el fin de ayudar a tomar decisiones informadas. Disponible en: [https://www.appcivico.com/historias-de-sucesso/voto-legal]. Acceso: 02.09.2024.

[12] En España, por ejemplo, la empresa Chocolate diseñó *Elecciones.chat*, un *chatbot* y *voicebot* disponible para asistentes de voz como *Alexa*, así como WhatsApp, a través del cual los usuarios pueden conocer las diferentes plataformas gubernamentales mientras realizan las tareas del hogar (Suárez, 2024).

[13] En Brasil, el Tribunal Superior Electoral lanzó en 2020 un *chatbot* en colaboración con WhatsApp. En 2022, la solución, que también había sido reformulada con el fin de *desacreditar* la desinformación, fue utilizada por más de 6,2 millones de

independiente los datos de escrutinio y recuento, incluso mediante misiones de observación electoral (Yazbek, 2024), así como ayudar a las personas con dudas, por ejemplo, sobre los colegios electorales o la documentación necesaria para llevar a cabo el ejercicio cívico, mediante modelos de asistencia virtual con procesamiento de lenguaje natural[14] .

Por consiguiente, en términos generales, las soluciones de IA pueden reducir la posibilidad de fraude, disuadir a los agentes malintencionados de actuar y proteger la integridad democrática permitiendo reacciones proactivas, oportunas y precisas para evitar[15], eliminar o castigar determinadas anomalías en aspectos clave de la organización de las elecciones (Chennupati, 2024; Stevenson, 2024).

Es importante señalar, dentro de este razonamiento, que el fraude, el abuso y la manipulación existen, pero no son las únicas ni las más destacadas formas de explotación de la inteligencia artificial en el contexto de las elecciones (Jungherr; Rauchfleisch; Wuttke, 2023). Esta comprensión es esencial para que los gobiernos y las instituciones electorales no consoliden una comprensión limitada y refractaria que desaliente la inversión necesaria en innovaciones que puedan aprovecharse.

Gráficamente, el cuadro siguiente recopila un conjunto variado (y no exhaustivo) de usos positivos de la IA en los procesos electorales, según lo observado en todo el mundo. Cada posibilidad contribuye a algún fin relacionado con la integridad del proceso (inclusión de segmentos vulnerables[16], reducción de costos económicos, depuración de prácticas ilegales o antisociales, aumento del nivel ético de la competencia y facilitación del derecho de acceso a la información).

votantes, permitiendo el intercambio de más de 177 millones de mensajes. Se ha convertido así en uno de los mayores *chatbots* de la plataforma en todo el mundo (Tribunal Superior Eleitoral, 2023).

[14] Una plataforma creada por la Universidad Estatal de Campinas (Unicamp) en colaboración con la Universidad Estatal de Río de Janeiro (UERJ) utiliza la IA para comparar más de 60.000 programas de gobierno presentados en las elecciones municipales de Brasil. Con la herramienta, los usuarios pueden buscar y comparar propuestas sobre los temas que más les interesan, sin tener que revisar las propuestas completas de todos los candidatos (Soares, 2024).

[15] Para ello, existen herramientas capaces de ejercer una moderación preventiva, actuando para eliminar contenidos nocivos incluso antes de que se publiquen. Algunos ejemplos son las herramientas automatizadas de reconocimiento de imágenes con tecnología *hash*, como *PhotoDNA*, creada por Microsoft, que ayuda a detectar de antemano material de pornografía infantil, y *ContentID*, de Youtube, que escanea exhaustivamente el sistema, encontrando y eliminando vídeos con infracciones de derechos de autor (Fux; Fonseca, 2022).

[16] Kumar Chennupati (2024) advierte que: "las consideraciones de accesibilidad e inclusión deben preceder al uso de la IA en las elecciones. Algunos programas informatizados pueden excluir a personas por falta de alfabetización digital o de acceso a la tecnología. Para garantizar que todo el mundo tenga las mismas oportunidades de votar, debemos dar cabida a las personas que decidan no utilizar o no puedan manejar dispositivos informáticos. Las personas que ya están en desventaja, como los hablantes no nativos o las comunidades desfavorecidas, pueden verse aún más afectadas si los sistemas de IA perpetúan deliberadamente estereotipos culturales o lingüísticos". Por eso, entre otros factores, "es esencial tener en cuenta la diversidad artística y lingüística para garantizar un acceso y una comprensión equitativos".

Cuadro 3: Aplicaciones legítimas de la IA en las campañas electorales

Automatización realista de la locución •(inclusión)	Generación automática de subtítulos y subtítulos opcionales •(inclusión)	Biometría de voz e imagen para desmentir los deepfakes •(depuración)	Detección automatizada de contenidos desinformativos y dañinos •(depuración)
Detección automática de contenido no deseado (críticas, rumores y propaganda negativa) •(competitividad)	Seguimiento de la cobertura informativa (clipping) para detectar historias negativas •(competitividad)	Monitorización de grupos públicos en aplicaciones de mensajería, con tratamiento semántico de indicadores de repercusión (análisis de tendencias y sentimientos) •(competitividad)	Asistencia o desarrollo integral de plataformas de campaña •(competitividad)
Supervisar la legalidad de las campañas adversarias, incluida la detección de comportamientos no auténticos •(depuración)	Seguimiento y análisis del rendimiento digital de las agendas temáticas y de la evolución de los competidores •(competitividad)	Modelos predictivos para la optimización táctica (perfilado de indecisos, anticipación de temas influyentes) •(competitividad)	Modelos prescriptivos para la (re)orientación de los enfoques (georreferenciación de focos de rechazo, software de recomendación neurolingüística) •(competitividad)
Gestión automatizada de perfiles, grupos y canales en redes sociales (programación de puestos) •(economía)	Chatbots para el servicio al votante (Haga preguntas, recopile datos, detalle propuestas, fomente la participación, presente materiales de verificación de hechos). •(competitividad)	Minería de datos con fines lícitos •(competitividad)	Personalización de la publicidad lícita •(competitividad)
Producción sintética de publicidad positiva (jingles, eslóganes, tarjetas, etc.) •(economía)	Producción sintética de materiales	Documentos informativas/proposicionales (redacción de declaraciones, sesiones informativas para los debates, textos para el derecho de respuesta) •(competitividad)	Automatización del centro de llamadas •(economía)
Editar, corregir o mejorar contenido de audio, vídeo o imagen •(economía)	Sistemas de autodetección para revelar el uso irregular de la IA generativa por parte de los adversarios •(depuración)	Asistentes virtuales para la organización de tareas burocráticas (programación de pagos, control de legalidad contable) •(economía)	Aplicaciones cívicas para organizar la información y comparar alternativas en disputa •(derecho a la información)
	Sistemas de síntesis para facilitar la comprensión de la información política •(derecho a la información)		

Fuente: Rubio Núñez; Alvim; Monteiro (2024), con adiciones y adaptaciones.

3.2 La inteligencia artificial contra la democracia

Sin embargo, está claro que, en el lado negativo, la revolución tecnológica está remodelando el horizonte de la comunicación política, la industria de los medios de comunicación, la naturaleza del mercado de ideas y el patrón de consumo de información. En consecuencia, el panorama de la búsqueda de votos, la organización de los intereses colectivos, el comportamiento público y la dinámica de construcción (y deconstrucción) de la confianza social se han reajustado de forma claramente perjudicial. Las innovaciones más radicales se refieren, por un lado, a la progresiva incorporación de algoritmos por parte de las plataformas de recuperación de información (motores de búsqueda) y los medios sociales y, por otro, a la expansión acelerada de los sistemas de procesamiento del lenguaje natural y de inteligencia artificial generativa (IAGen), expertos en crear atajos para la producción de información inexacta.

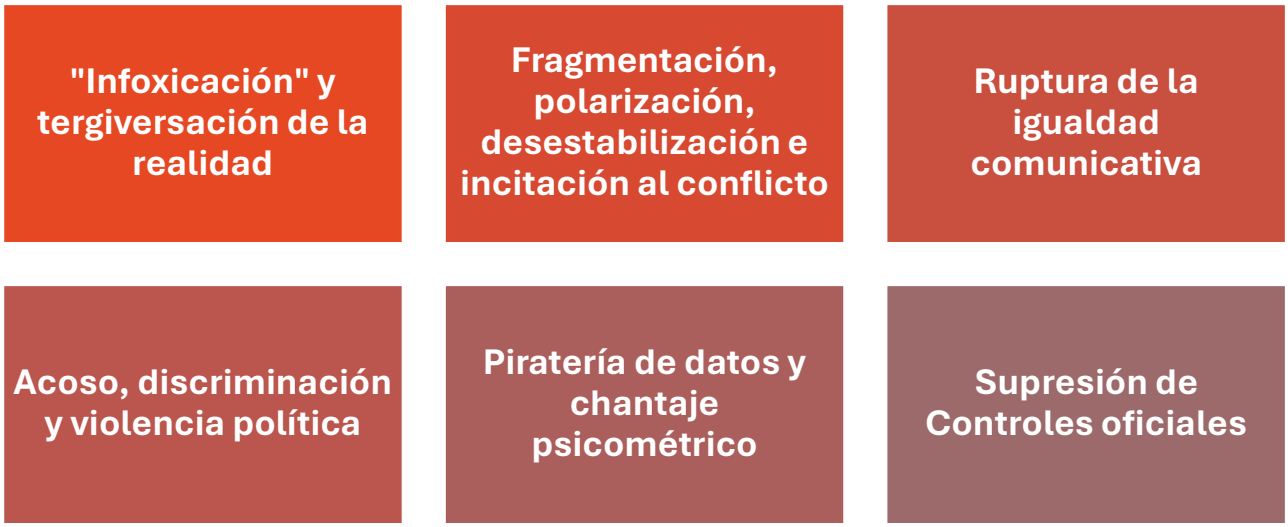
Además, estos elementos alteran radicalmente el ecosistema de producción de información, introducen nuevos actores en las discusiones públicas, empoderan a grupos malintencionados y ponen en peligro el orden jerárquico de credibilidad de las fuentes (Kavanagh; Rich, 2018), dando lugar a una esfera digital inflada, superficial, intolerante y hostil, en la que las opiniones se confunden con los hechos (Charaudeau, 2016). Dentro de este escenario, las narrativas desafían la realidad objetiva, la tecnología crea pruebas para afirmaciones falsas (Filimowicz, 2022) y las personas, paradójicamente, "ya no creen en nada y, al mismo tiempo, son capaces de creer en cualquier cosa" (Grijelmo, 2017).

Estas cuestiones aumentan en gran medida la disponibilidad, receptividad y modos de producción, distribución e intercambio de "discursos corrosivos" (Zachary, 2020), incluida la defensa de agendas antidemocráticas y narrativas de desinformación.

El panorama muestra que la IA facilita a cualquiera la creación y difusión de contenidos nocivos, lo que la convierte en "una herramienta especialmente peligrosa para la democracia cuando se utiliza de mala fe" (Denemark, 2024). La desinformación generada por la inteligencia artificial, en particular, fue clasificada recientemente en un informe del Foro Económico Mundial como el "principal riesgo emergente" en los próximos dos años (Foro Económico Mundial, 2024), y el avance increíblemente rápido de esta tecnología sugiere que el panorama de las actividades dañinas a menudo se renueva, yendo más allá de la mera sofisticación de antiguos trastornos bien conocidos (Hawes; Hall; Ryan, 2023).

Considerando sus efectos directos e indirectos, Rafael Rubio, Frederico Alvim y Vitor Monteiro (2024) consideran que, en el contexto de las campañas electorales, las soluciones inteligentes instrumentalizan una amplia gama de comportamientos indeseables capaces de socavar el marco de derechos y libertades básicos para unas elecciones honestas, justas y libres. Estos comportamientos han sido sistematizados en diferentes categorías que, en conjunto, conforman un modelo taxonómico segmentado en seis frentes:

Figura 1: Taxonomía de los trastornos de la información basados en la IA



Fuente: Rubio Núñez; Alvim; Monteiro (2024).

A continuación, se analizarán las prácticas relacionadas, tomando como referencia central el marco teórico referido.

A. “Infoxicación” y tergiversación de la realidad

Las prácticas de alteración de la realidad implican la automatización de procesos y la distribución masiva *de fake news*, *cheapfakes*, *deepfakes*, rumores y otras falsas narrativas, así como la creación de falsos movimientos de opinión en comunidades virtuales (*astroturfing*), basados sobre todo en comportamientos inauténticos llevados a cabo por robots que perturban e influyen en procesos sociales sensibles. Al mismo tiempo, la

inteligencia artificial puede obstruir el acceso a cuestiones importantes y a la realidad de los hechos sobrecargando la información mediante herramientas de difusión masiva *(spreaders*, *spambots*) y cuentas automatizadas utilizadas para difundir elementos de distracción (cortinas de humo) o campañas intensivas de desinformación *(firehosing*). Además, las alucinaciones de la IA[17], aunque sean accidentales, pueden dañar significativamente el panorama informativo, poniendo en peligro las elecciones (Rubio Núñez; Alvim; Monteiro, 2024).

Como prueba del evidente potencial de IAGen para llevar a cabo campañas encubiertas de injerencia, la empresa OpenAI reveló recientemente el descubrimiento del uso malicioso de su plataforma en cinco operaciones de desestabilización llevadas a cabo sistemáticamente por actores extranjeros[18]. Utilizando la herramienta ChatGPT para generar y traducir artículos de noticias y comentarios breves que alimentaban cuentas falsas, los operadores de la trama buscaban influir en los debates públicos en torno a determinadas agendas en las redes sociales (Carrascón, 2024).

B. Fragmentación, polarización, desestabilización e incitación al conflicto

Desde esta perspectiva, las mismas herramientas utilizadas para producir desinformación pueden servir para diseñar, publicar y viralizar otro tipo de discursos dañinos, utilizados como palanca para movilizar a segmentos de la población que se sienten engañados, traicionados o excluidos. Desde este punto de vista, la inteligencia artificial alimenta la explotación política del odio y la desconfianza, reforzando comportamientos agresivos e intolerantes contra grupos minoritarios o vulnerables, corrientes ideológicas contrarias o instituciones electorales. Junto a las narrativas engañosas, por tanto, las soluciones inteligentes pueden movilizarse para difundir contenidos extremistas y radicales, con fuertes repercusiones negativas en el proceso electoral (Rubio Núñez; Alvim; Monteiro, 2024).

[17] Las alucinaciones se producen cuando los modelos generativos de IA, debido a algún fallo, fabrican respuestas o anotaciones que parecen fiables, pero son falsas (Panditharatne; Giansiracusa, 2023). Por ejemplo, una investigación llevada a cabo por la organización AI Democracy Projects en la que participaron cinco modelos de *chatbot* diferentes concluyó que las consultas sobre temas electorales devolvían resultados falsos o inexactos en el 50% de los intentos (Soon; Quek, 2024).

[18] Las cinco operaciones detectadas incluían a) una operación rusa dirigida a Ucrania, los países bálticos y Estados Unidos, centrada en la creación de comentarios con motivaciones políticas para su distribución en la app Telegram ("Operación *Mala Gramática*") b) una iniciativa rusa para producir comentarios en varios idiomas, utilizando plataformas como X y 9GAG para su difusión ("Operación *Doble"*); c) una red china que utilizaba IA para crear textos en varios idiomas y gestionar plataformas en línea (Operación *"Spam Camouflage*"); d) un plan iraní que producía y traducía artículos extensos para su publicación en sitios web afiliados (Operación "*Unión Internacional de Medios Virtuales*" - IUVM); y e) una empresa comercial israelí que creaba artículos y comentarios para plataformas de medios sociales como Instagram, X y Facebook (Operación "*Zero Zeno"*) (Matoruga, 2024).

Los algoritmos de las redes sociales, en particular, son en gran medida responsables del "apogeo de la polarización" (Vivas Escribano, 2023), que a menudo se gesta en cámaras de eco que refuerzan, retroalimentan y potencian antipatías, animadversiones y prejuicios negativos que inducen fuertes divisiones sociales. Según diversos estudios, las comunidades virtuales cristalizan identidades y crean barreras entre grupos políticos, facilitan la hiper emocionalidad ideológica y, en consecuencia, profundizan las fracturas políticas y sentimentales, estimulando la circulación de mensajes que evocan sentimientos de ira y repugnancia (López-Ponce; Barredo-Ibáñez; Sánchez Gonzales, 2024) con efectos altamente contagiosos entre la población (Martinez-Brawley, 2024).

C. Violación de la igualdad comunicativa

En las redes sociales, la inteligencia artificial, en combinación con otras tecnologías digitales (como la técnica del disparo masivo), perfila el marco general de ideas y opiniones que llegarán a cada usuario, diseñando la ventana a través de la cual los usuarios contemplan el mundo. Dado que seleccionan todo lo que será visto o ignorado -y con qué fuerza circulará cada mensaje-, los algoritmos de priorización y recomendación de contenidos desempeñan un papel importante en la formación de creencias y en la consolidación de las opciones electorales (Rubio Núñez; Alvim; Monteiro, 2024).

Al mismo tiempo, la moderación automatizada de contenidos afecta también al panorama general de la comunicación en red, lo que puede llevar a la eliminación o reducción sistemática del alcance de determinados temas, a la reducción de la credibilidad de ciertas afirmaciones (con la inserción de etiquetas, marcas o pantallas de advertencia, señalando la existencia de contenidos falsos o dudosos, por ejemplo) y, en última instancia, a la exclusión de ponentes o grupos de discusión, como resultado de decisiones de suspensión o prohibición por la supuesta violación, reiterada o no, de las normas de la comunidad o de políticas relacionadas (Oliva; Tavares; Valente, 2020). Aunque existen algoritmos de aprendizaje masivo, al menos en teoría, para reconocer contenidos problemáticos de forma libre de sesgos humanos (Gillespie, 2018), lo cierto es que las técnicas computacionales toman decisiones con fuertes implicaciones sociopolíticas.

La presencia de imprecisiones o sesgos en las herramientas basadas en grandes modelos lingüísticos (LLM) también puede afectar a la calidad del panorama informativo, generando distorsiones que inciden en la dimensión política de la opinión pública. La provisión de respuestas sesgadas o incorrectas por parte de las soluciones generativas crea retos adicionales en términos de eliminación de sistemas de privilegio, que pueden

favorecer ciertas inclinaciones ideológicas en detrimento de otras (Rotaru; Anagnoste; Oancea, 2024), afectando al equilibrio esperado entre los polos.

A la luz de lo expuesto, exigir neutralidad partidaria en las plataformas digitales cobra importancia, dado que el principal espacio de desarrollo de la política hoy está dominado por grandes empresas tecnológicas que, al imponer términos y condiciones obtienen la capacidad de aplicar pautas privadas al "juzgamiento" de casos concretos y ejercen facultades "cuasi legislativas", "cuasi judiciales" (Fux; Fonseca, 2022) y "cuasi-gubernamentales" (Cupać; Schopmans; Tuncer-Ebertürk, 2024), con graves consecuencias para la competición electoral.

D. Acoso, discriminación y violencia política

Del mismo modo que las redes conectan a personas que se conocen y se caen bien, o que comparten creencias y gustos similares, éstas también reúnen a individuos y grupos que piensan y opinan de forma diferente, ya sea sobre cuestiones menores, en principio triviales, o sobre aspectos sensibles, controvertidos y de gran relevancia. En este contexto, así como las comunidades virtuales albergan usuarios comprensivos, tolerantes y cordiales con la disonancia, también albergan legiones de individuos intolerantes, provocadores e incivilizados, afectos y prácticas antidemocráticas y antisociales, expresadas en diferentes formas de discriminación, acoso y violencia política (Rubio Núñez; Alvim; Monteiro, 2024), muchas veces estimulados por un pernicioso esquema de gratificación, materializado en aplausos digitales encontrados en emojis, botones sociales o comentarios viscerales de aliento.

En este ambiente, preocupa un "desplazamiento sistemático de las fronteras comunicativas, especialmente en detrimento de grupos vulnerables cuyos derechos [políticos y] de la personalidad se ven amenazados", así como el hecho de que estas manifestaciones pongan en peligro "las reglas fundamentales de un discurso abierto de ciudadanos libres e iguales en una sociedad democrática" (Eifert, 2022). Las minorías expuestas son, al mismo tiempo, víctimas perpetuas de una persecución hostil y objeto monotemático de tácticas manipuladoras que rebajan su dignidad mediante invenciones, exageraciones y generalizaciones, administradas para manipular la opinión de los exogrupos a través de fantasiosas narrativas de amenazas existenciales, oxígeno para la cultura del odio y la política del miedo.

La incidencia recurrente del trolling produce un efecto de normalización de los discursos ilegítimos, que, a través de la repetición no reprimida, acaban ganando una

reserva cautiva en los espacios de discusión, como resultado de un fenómeno de comunicación conocido como la "ventana de Overton". A través de la recurrencia, la abundancia y la aceptación tácita (y a veces explícita), los ataques identitarios se (re)instalan en el paisaje social, como si formaran parte de él, como si a través de alguna visión distorsionada de la ley (el espantajo creado por el absolutismo libertario de la expresión) pudieran permanecer allí.

E. Piratería de datos y chantaje psicométrico

La digitalización de los negocios, de las transacciones comerciales, de la circulación de la información, de los servicios públicos y de las interacciones humanas en términos individuales y colectivos ha transportado una enorme cantidad de datos a la dimensión de la red, estableciendo la materia prima necesaria para que los algoritmos decodifiquen los engranajes del mundo y entren en juego como un modelo de negocio que revoluciona las dimensiones de la publicidad electoral (Rubio Núñez; Alvim; Monteiro, 2024).

Los modelos de “big data” ayudan a candidatos, partidos políticos y actores malintencionados a leer la mente de los votantes y ver patrones de comportamiento, correlaciones invisibles y otras *percepciones* con una claridad increíble (Safiullah; Parveen, 2021). En estas condiciones, la propaganda se vuelve mucho más eficaz y precisa, llegando a las personas adecuadas en el *momento* oportuno (Hawes; Hall; Ryan, 2023), dada la capacidad de detectar momentos de vulnerabilidad o mayor susceptibilidad personal o de grupo (Tavares, 2022).

F. Supresión de los controles oficiales

Por sus características, la arquitectura de redes se apoya en la economía, la ubicuidad, la facilidad de acceso, la rapidez y, sobre todo, la falta de control previo y el anonimato para aglutinar a un enorme conjunto de usuarios dados a comportamientos nefastos y prácticas que vulneran derechos fundamentales (Herrerías Castro, 2023). La IA también juega un papel en estas cuestiones, ya que la computación inteligente posibilita los ciberataques a distancia, además de aportar soluciones que debilitan el sistema de rendición de cuentas al añadir capas de impunidad y anonimato (Rubio Núñez; Alvim; Monteiro, 2024), además de que muchas de las disfunciones comentadas tienden a producirse de forma silenciosa y subrepticia, por no decir invisible. Los riesgos, desde esta

perspectiva, acaban ampliándose debido a la desproporcionada relación entre la cuantía del premio y los posibles inconvenientes para los sujetos en acción (Vacarelu, 2023).

Es más, los actores maliciosos que invierten en IA para aprovechar la desinformación son "altamente adaptables, refinando continuamente sus estrategias para evitar ser detectados". A medida que las plataformas implementan nuevas defensas y tecnologías de identificación, estos actores encuentran nuevas vulnerabilidades que explotar, o desarrollan modelos inteligentes aún más sofisticados para eludir los filtros. Este "continuo juego del gato y el ratón" representa un reto importante en la búsqueda de soluciones eficaces y duraderas capaces de mitigar eficazmente los contenidos nocivos impulsados por la IA (Yu, 2024).

4. Premisas para entender el debate reglamentario

En términos generales, el concepto de regulación engloba la idea de ordenar las actividades económicas con el fin de garantizar que dichas actividades se lleven a cabo en armonía con determinados objetivos sociales, más allá de los estrictos intereses del mercado respectivo. Aunque la regulación se ha entendido tradicionalmente como una concertación de actividades económicas, la noción se aplica también al contexto de la regulación social, entendiendo por tal una intervención que no tiene por objeto inmediato la regulación de un mercado, sino de aspectos del comportamiento de sujetos que operan en un determinado ámbito jurídico y que son relevantes desde una perspectiva colectiva. Desde este ángulo, el tratamiento de las redes sociales y sus algoritmos implica un debate reglamentario, dado que estas redes centralizan un mercado publicitario y un mercado de tráfico de información, así como el mercado de intercambios e interacción entre usuarios (Farinho, 2022).

Aunque Internet suele tener diferentes capas - a) la capa de infraestructura; b) la capa de código; c) la capa de aplicaciones; y d) la capa de contenidos, según la definición seminal de Lessig (1999)-, lo cierto es que, en sus intersecciones con la materia electoral, las pretensiones regulatorias suelen concentrarse en las dos últimas. Dentro de este ámbito, las normas establecidas tienden, por lo general, a prescindir de consideraciones sobre supuestos de equipamiento e infraestructuras, como los cables de fibra óptica, así como de detalles relacionados con la interoperabilidad de las redes y los protocolos de conexión y navegación, para centrarse en aspectos relacionados con la gobernanza y el

funcionamiento de las plataformas digitales, así como con el conjunto de publicaciones que reciben, ponen a disposición y aprovechan.

Los últimos ciclos electorales demuestran que "el auge de la inteligencia artificial ha cambiado las condiciones en las que la sociedad se comunica y genera conocimiento", aportando novedades que desafían y a la vez exigen un movimiento normativo con respuestas institucionales (Vesting, 2022). La preocupación normativa en este segmento tiende a evitar que el "control de las reglas del juego" que proporcionan las tecnologías digitales descienda a un exacerbado "grado de alienación" respecto de los valores y principios rectores del derecho (Tavares, 2022), a fin de asegurar que las contiendas electorales absorban las transformaciones tecnológicas manteniendo su esencia democrática. En otras palabras, para asegurar que las nuevas tecnologías se ajusten a los estándares democráticos, y no que la democracia se someta al modelo de negocios de las nuevas tecnologías.

A pesar de compartir un objetivo común, lo cierto es que los distintos ordenamientos jurídicos no siguen necesariamente el mismo camino, dado no sólo el peso de las diferencias relativas a la tradición histórica y la cultura jurídica, así como las presiones y contingencias que afectan al clima y la voluntad política y social, sino (también) la aparición casi simultánea de un variado arsenal de posibles enfoques que añade una capa adicional de complejidad (Bozkurt, 2024) a la ya ardua tarea de elegir. A modo de ejemplo, el estado actual de la técnica ofrece a las autoridades y gobiernos interesados la posibilidad de invertir, alternativamente a) en declaraciones de principios y normas éticas; b) en la adaptación de la normativa existente, tratando de adecuarla al contexto de la IA y proponiendo nuevas formas de abordar los retos específicos de la tecnología; c) en el diseño de estrategias gubernamentales para la regulación de la IA, incluyendo la creación de agencias reguladoras, la implementación de políticas públicas y el fomento de la investigación y el desarrollo responsables; y d) la creación de modelos estructurados que orienten el desarrollo, la implantación y el uso de la IA, combinando principios éticos con recomendaciones prácticas y mecanismos de gobernanza basados en *marcos* y directrices (Almeida; Santos; Farias, 2021).

En cuanto a las cuestiones de fondo, el contenido normativo dependerá de "opciones tomadas a partir de deliberaciones políticas y sociales entrelazadas con la cultura, el desarrollo histórico y el propio Derecho de cada nación soberana" (Fux; Fonseca, 2022), especialmente en lo que se refiere a las diferentes visiones sobre la dicotomía libertad de expresión *versus* protección de la integridad o legitimidad de las elecciones, lo que, a estos efectos, traslada las viejas discusiones sobre el papel (débil o poderoso) del Estado en la

orientación de la sociedad a la dimensión de la gobernanza de las redes (Fachin; Veronese, 2024).

En este contexto, la escisión entre sistemas libertarios y proteccionistas, junto con los diferentes grados de riesgo y exposición a prácticas antidemocráticas, contestatarias y golpistas, da lugar a la aparición de sistemas más contenidos (modelos minimalistas) por un lado y sistemas más completos (modelos maximalistas) por otro, dotados de un mayor sentido de la intervención como resultado de un compromiso tácito con una noción de democracia sustantiva, combinada con la idea de democracia militante[19]. Estas mismas circunstancias hacen también "natural y esperable" que se produzcan "fricciones" ocasionales entre las tecnologías globales y algunas regulaciones locales (Estarque; Archegas, 2021).

Comprender la importancia de la IA en las elecciones requiere ser consciente de las muchas visiones y problemas que existen en los distintos países y lugares. Las naciones tecnológicamente maduras suelen tener una comprensión más matizada de los peligros de la IA (Chennupati, 2024), lo que tiende a reflejarse en una mayor capacidad para regular las tecnologías basándose en un pensamiento propio, independiente y adecuado a la situación. Mientras tanto, en los entornos menos desarrollados, un menor conocimiento fomenta la importación pura y simple de modelos extranjeros.

El gran problema es que, en el ámbito de las reformas electorales, los efectos de los dispositivos varían necesariamente en función de las condiciones sociopolíticas del entorno en el que se aplican. Desde esta perspectiva, el éxito aparente de un modelo en un lugar determinado no garantiza el éxito absoluto en el escenario nacional, ya que la experiencia

[19] Desde esta perspectiva, cabe recordar "[...] el diferente peso que se concede a la libertad de expresión en los distintos modelos de democracia. El término se utiliza para describir una variedad de modelos de organización del Estado y, por lo tanto, es posible identificar diferentes ejes a lo largo de los cuales varían los modelos de democracia. Dos de ellos merecen ser destacados [...] por su influencia en el papel atribuido a la libertad de expresión. El primero clasifica las democracias en sustantivas o procedimentales. Estas últimas se preocupan por garantizar procedimientos democráticos formales, como elecciones periódicas y libres, sin entrar en consideraciones cualitativas sobre los resultados de estos procedimientos. Las democracias sustantivas, en cambio, se preocupan no sólo de los procedimientos formales, sino también de los resultados producidos. Por lo tanto, son importantes consideraciones como garantizar la igualdad material de todos los grupos. En este contexto, las democracias procedimentales tienden a valorar la libertad de expresión por sí misma, basándose en la percepción de que es esencial para la subsistencia y la legitimidad de los procedimientos democráticos formales. Las democracias sustantivas, por otro lado, tienden a permitir una mayor interferencia del Estado en el discurso, con el objetivo de promover resultados sustantivos específicos. [...] El segundo eje implica la gradación entre democracias libertarias y militantes. El principal elemento que distingue estas categorías es la libertad concedida al discurso y a las organizaciones que se oponen y amenazan las propias estructuras democráticas que hacen posible el autogobierno. Por un lado, las democracias libertarias conceden sólidas protecciones también a este tipo de discurso, permitiendo la regulación sólo a partir del punto en que el discurso se convierte en una amenaza inminente de violencia política. [...] Por otro lado, las democracias militantes permiten restricciones al discurso o a la existencia de grupos (por ejemplo, partidos políticos) que atacan a las instituciones democráticas, incluso cuando no existe un riesgo inminente de violencia política. Y esto no sólo para proteger a las democracias de posibles ataques violentos, sino también para protegerlas de la posibilidad de subversión por medios democráticos, como ocurrió, por ejemplo, con el ascenso del partido nazi en Alemania en 1933, elegido por un proceso electoral legítimo" (Barroso, 2023).

demuestra que modelos idénticos suelen tener resultados diferentes en distintos países (Meirinho Martins, 2015). Cuando se trata de sistemas electorales, el contexto marca la diferencia (Nohlen, 2015), de modo que una misma disposición puede, como es lógico, tener efectos políticos radicalmente distintos cuando se aplica en entornos diferentes. De ahí la conclusión de que la importación de modelos extranjeros debe ir precedida de un diagnóstico exhaustivo de la situación económica del país.

5. Estudios de casos sobre experiencias normativas con la IA en las elecciones

El marco regulador del uso de la IA en los procesos electorales es bastante incipiente, mostrándose limitado y tímido ante los inmensos retos que plantean estas tecnologías. Aunque varias instituciones internacionales ya han trabajado para crear marcos de protección democrática adaptados a este nuevo contexto, la regulación electoral sigue dependiendo en gran medida de la iniciativa autorreguladora de los proveedores de tecnología, que la experiencia ha demostrado bastante insuficiente (Rubio Núñez; Alvim; Monteiro, 2024).

En este sentido, es imprescindible crear un marco institucional que regule el impacto de la IA en las elecciones, con el fin de garantizar la protección de los derechos democráticos y orientar la búsqueda de una neutralidad tecnológica mimética, basada en la promoción de la seguridad, la transparencia, la auditabilidad y "explicabilidad" y la no discriminación, entre otros valores en cuestión.

En las siguientes líneas se presentan algunas de las iniciativas normativas adoptadas en todo el mundo.

a. Brasil

Brasil celebra una de las mayores elecciones tecnológicas del mundo, con más de 155 millones de votantes y un número de urnas electrónicas que asciende a más de 500.000 unidades. El Tribunal Superior Electoral (TSE) del país ha sido pionero en el uso de sistemas de voto electrónico desde 1996. Sin embargo, en un contexto de creciente polarización política y de intensa contaminación del ecosistema informativo (Rubio Núñez; Monteiro, 2023), Brasil ha enfrentado importantes desafíos para mantener la confianza social en el sistema de justicia electoral, en las máquinas de votación y en las propias elecciones. En este contexto, las posibilidades derivadas del uso de sistemas de

inteligencia artificial en los procesos electorales obligan al país a prepararse para nuevos retos.

En Brasil, todavía no existe una legislación formal específica para el uso de la inteligencia artificial en general. No obstante, en el Parlamento se están debatiendo iniciativas reguladoras, como el proyecto de ley 21/2020, cuyo objetivo es "permitir el desarrollo y la aplicación de IA segura y fiable, en consonancia con los valores y principios de la Constitución Federal". En general, el proyecto de ley se basa en tres pilares fundamentales: a) garantizar un conjunto de derechos a las personas directamente afectadas por los sistemas de IA; b) categorizar los niveles de riesgo asociados a estos sistemas y a los algoritmos basados en esta tecnología; y c) implementar medidas de gobernanza para las empresas y organizaciones que proporcionan u operan dichos sistemas (Rubio Núñez; Alvim; Monteiro, 2024).

La falta de un marco regulatorio específico sobre inteligencia artificial (IA) y desinformación, sumada al riesgo inminente que el uso inadecuado de estos recursos representa para los procesos electorales, ha colocado al Tribunal Superior Electoral (TSE), encargado de organizar las elecciones y juzgar los conflictos derivados de ellas, como protagonista en la adopción de medidas regulatorias. Haciendo uso de la prerrogativa prevista en el artículo 57-J de la Ley Electoral (Ley 9.504/97), el Tribunal Superior aprobó un conjunto inédito de disposiciones para regular el uso de sistemas inteligentes en las campañas. Por medio de la Resolución 23.732/2024, se modificó profundamente la reglamentación de la propaganda electoral, Resolución 23.610/2019, con la inclusión de los artículos 9-B a 9-H, que tratan específicamente del uso de IA en las elecciones brasileñas.

La nueva resolución permite expresamente el uso de inteligencia artificial generativa en la producción de contenidos, además de autorizar el uso de soluciones de inteligencia sintética para mejorar, modificar o adaptar materiales de comunicación (art. 9-B). La norma permite explícitamente el uso de IAGen en la creación completa de contenidos, la modificación de elementos estéticos, sonoros o textuales, la eliminación de componentes vocales o visuales, la combinación de audio e imágenes, el ajuste de la velocidad de reproducción, la superposición de grabaciones (por ejemplo, integrando una grabación de estudio con otra externa) o sonidos (como priorizar la voz de un locutor sobre otra simultáneamente).

Con el fin de mejorar la transparencia en el uso de la IA en las elecciones, se exigió, como norma general, que cualquier contenido sintético, ya sea parcial o total, vaya acompañado de una advertencia explícita - "destacada y accesible"-, con el objetivo de garantizar que el público no sea inducido a error sobre el origen o la naturaleza del material

presentado. En este sentido, la normativa del TSE, en el uso de su poder reglamentarios, sigue las directrices establecidas en un informe de la Comisión Europea, que subraya la importancia de la transparencia para mitigar el riesgo de manipulación (Denemark, 2024).

La norma establece cómo debe realizarse la *advertencia* sobre el uso de IA (§1), de la siguiente forma: a) al inicio de las piezas o comunicaciones realizadas mediante audio; b) mediante etiquetado (marca de agua) y en la audiodescripción, en las piezas consistentes en imágenes estáticas; c) en la forma prevista en los puntos *a* y *b,* en las piezas o comunicaciones realizadas mediante vídeo o audio y vídeo; d) en cada página o cara del material impreso en el que se utilicen contenidos producidos mediante inteligencia artificial. La resolución prevé algunas situaciones en las que se exime del deber de advertencia, como en el caso de a) las alteraciones que sólo sirvan para promover una mejor calidad de imagen y sonido, b) la inclusión de elementos de identidad visual, viñetas o logotipos, y c) los recursos habituales de edición de imágenes que promuevan montajes en los que aparezca el candidato junto a simpatizantes. La lógica detrás de esta disposición descansa en la idea de que estas situaciones no tienen el poder de engañar al votante, para no configurarse como un "determinante cognitivo del voto" (Rubio Núñez; Alvim; Monteiro, 2024). Por lo tanto, los excesos en el uso de estos recursos, como el uso de técnicas *de de-aging* (rejuvenecimiento artificial) y *makeover* (cambio visual profundo)*, hacen* obligatoria la advertencia sobre el uso de IA, según las normas brasileñas.

Otra disposición importante se refiere a la autorización expresa para el uso de *chatbots* y avatares en las campañas, que también exige la presentación de un *descargo de responsabilidad* sobre el uso del recurso (§3). Para evitar dudas y engaños, la normativa prohíbe la simulación de diálogo con cualquier ser humano, candidato o no. El incumplimiento de esta disposición impone la retirada inmediata del contenido y la indisponibilidad del servicio, ya sea por iniciativa del proveedor de la aplicación o por orden judicial (§4).

En cuanto a la utilización de contenidos producidos sintéticamente o manipulados para generar desinformación, la resolución prohíbe expresamente su uso en cualquier tipo de propaganda electoral con potencial para impactar en la igualdad de la contienda, causando daño al equilibrio de las elecciones o a la integridad del proceso electoral (9º-C). Al referirse a la preservación de la integridad electoral, la norma extiende la prohibición del uso de IA para producir desinformación no sólo a los candidatos, sino también contra las instituciones electorales y las autoridades que las integran.

Otro aspecto relevante se refiere al tratamiento de las plataformas digitales. Debido a la insuficiencia de las medidas de autorregulación adoptadas por *las grandes tecnológicas*

para contener la propagación pandémica de contenidos desinformativos en elecciones anteriores, y a la reciente experiencia de graves ataques antidemocráticos en el país (que culminaron en el intento fallido de golpe de Estado del 8 de enero de 2023), la resolución exige ahora a las empresas tecnológicas que adopten medidas más concretas relacionadas con el *deber de diligencia* y la función social de las plataformas.

En este sentido, estableció la obligación de los proveedores de adoptar y publicar medidas para "impedir o reducir la circulación de hechos notoriamente falsos o gravemente descontextualizados" que tengan la potencialidad de afectar el trámite regular de la elección (9º-D). También prohibió a los proveedores de aplicaciones lucrar con la difusión de desinformación que afecte al proceso electoral, prohibiendo la comercialización de cualquier forma de promoción, incluso priorizanr resultados de búsqueda para la difusión de contenidos de esta naturaleza (§1, 9º-D).

Además, se impuso a las plataformas la obligación, con independencia de una decisión judicial, de adoptar las medidas necesarias para poner fin a la promoción, monetización y acceso a publicaciones que contengan desinformación contra la integridad del proceso electoral. Lo que se aprecia aquí es la construcción de reglas dirigidas a promover un comportamiento proactivo y transparente por parte de las plataformas, orientado a mitigar los efectos nocivos de la desinformación digital sobre el entorno democrático y las contiendas electorales.

Aunque algunos puntos puedan ser cuestionados, como el carácter excesivamente genérico de algunas de las obligaciones impuestas, la solución normativa responde a una gran necesidad, desencadenando un mecanismo sancionador capaz de exigir un comportamiento responsable a las plataformas digitales, a través del establecimiento de un deber de cuidado, cuyo incumplimiento significaría una "omisión legal relevante" (Rubio Núñez; Alvim; Monteiro, 2024) en la aplicación de la ley electoral.

En este marco, la resolución estipula, en una lista abierta, algunos ejemplos de comportamiento deseable y esperado en las plataformas de medios sociales:

- Redacción de condiciones de uso y políticas de contenidos compatibles con el objetivo establecido.
- Implementación de herramientas de notificación eficaces y canales de información accesibles, tanto para los usuarios como para las instituciones públicas y privadas.
- Planificación y ejecución de acciones correctivas y preventivas, mejorando los sistemas de recomendación de contenidos.

- Transparencia de los resultados obtenidos por las acciones de planificación y ejecución, especialmente en relación con las acciones correctivas y preventivas.
- Evaluación del impacto de sus servicios en la integridad del proceso electoral, centrándose en la aplicación de medidas eficaces para mitigar los riesgos, incluida la violencia política de género.
- Mejorar las capacidades tecnológicas y operativas, dando prioridad a las herramientas que contribuyan a reducir la desinformación (art. 9d).

Al tratar asuntos más sensibles a la salud democrática, la resolución brasileña trasladó la lógica de la regulación asimétrica en función de la magnitud de los riesgos para la disciplina electoral (Bioni; Garrote; Guedes, 2023), muy común en las regulaciones sobre el uso de IA en todo el mundo (Rubio Núñez; Alvim; Monteiro, 2024).

En este punto, el marco brasileño (art. 9-E) fue aún más incisivo al establecer la responsabilidad solidaria de las plataformas digitales, en las esferas civil y administrativa, cuando no promuevan, durante el período electoral, la eliminación sumaria de contenidos y cuentas que representen un riesgo: I) de conductas, informaciones y actos que puedan caracterizar delitos que impacten particularmente el ambiente democrático, tales como la abolición violenta del Estado Democrático de Derecho, golpe de Estado, interrupción del proceso electoral, violencia política, entre otros; II) de la divulgación o compartición de hechos notoriamente falsos o gravemente descontextualizados que afecten la integridad del proceso electoral, incluyendo los procesos de votación, escrutinio y cómputo de votos; III) amenazas graves, violencia o incitación a la violencia física contra los miembros y el personal de la Justicia Electoral y del Ministerio Público Electoral o contra la infraestructura física del Poder Judicial con el fin de restringir o impedir el ejercicio de los poderes constitucionales o la abolición violenta del Estado Democrático de Derecho; IV) comportamiento o discurso de odio, incluida la promoción del racismo, la homofobia, las ideologías nazis, fascistas o de odio contra una persona o grupo debido a prejuicios de origen, raza, sexo, color, edad, religión y cualquier otra forma de discriminación; V) la difusión de contenidos sintéticamente fabricados o manipulados, incluso por AI, en desacuerdo con las normas de etiquetado establecidas en la resolución.

A pesar de las buenas intenciones mostradas al pretender reforzar el régimen de responsabilidad de las plataformas por los contenidos producidos en su entorno digital, lo cierto es que, tal como se presenta, la norma asigna a los particulares la tarea de realizar un escrutinio "extremadamente técnico e innegablemente propio de las funciones del Estado-juez", además de parecer chocar con la disposición general sobre responsabilidad

prevista en la Ley nº 12.965/2014, que establece el Marco de Derechos Civiles en Internet (Rubio Núñez; Alvim; Monteiro, 2024), según la cual las plataformas sólo son responsables de los contenidos de terceros en caso de negativa a cumplir órdenes judiciales específicas, dentro del plazo especificado y de acuerdo con sus capacidades técnicas.

Asimismo, cabe destacar que los cambios introducidos en la Resolución 23.610 también sirvieron para reforzar el marco jurídico de la protección de datos en Brasil. Esto es especialmente relevante dado que la cuestión del tratamiento de datos en contextos electorales no ha sido regulada ni por la Ley General de Protección de Datos brasileña ni por la legislación electoral (Rubio Núñez; Alvim; Monteiro, 2024). Sobre el tema, el §4 del art. 10 establece que el tratamiento de datos debe cumplir la finalidad para la cual los datos fueron recogidos, y que deben observarse los principios y reglas de la Ley General de Protección de Datos (LGPD). También estipula que los agentes electorales deben proporcionar información clara sobre el tratamiento de los datos personales y crear canales para que los votantes puedan solicitar la supresión o la baja (art. 10, § 5). También en esta línea, el §9 del art. 28 estipula que deben observarse las normas de la LGPD para la propaganda electoral que implique el tratamiento de datos personales sensibles.

Aunque todavía es demasiado pronto para sacar conclusiones definitivas sobre los resultados prácticos de la normativa brasileña sobre el uso de la IA, es posible identificar que la arquitectura normativa adoptada refleja la breve (pero profunda) experiencia que el sistema electoral del país ha tenido en la lucha contra la desinformación en las campañas digitales y las soluciones innovadoras, ágiles y exitosas que ha ideado para garantizar la integridad de su proceso electoral.

b. Estados Unidos

En Estados Unidos, el uso de la IAGen ha sido recurrente en campañas desinformativas en las elecciones presidenciales, incluyendo *robocalls* imitando la voz del presidente Biden y fotos inventadas del expresidente Donald Trump siendo arrestado. Casos como estos plantean dudas sobre los límites de estas herramientas en contextos electorales, y suponen una parte importante del debate sobre la IA en las elecciones.

A finales de julio de 2024, se habían registrado en suelo estadounidense 151 proyectos de ley sobre *deepfakes* y medios de comunicación engañosos en el contexto electoral (Norden; Narang; Protzmann, 2024). Esta cifra representa alrededor de una cuarta

parte de todos los proyectos de ley presentados sobre el tema general de la inteligencia artificial en el país. En general, estas normativas pretenden regular la desinformación contra los candidatos o los comportamientos que influyen indebidamente en los votantes.

En los últimos años se han aprobado varias leyes estatales sobre el uso de *deepfakes.* Mientras que algunas de estas leyes prohíben absolutamente el uso de recursos *deepfake* y otros medios engañosos en las campañas electorales, otras permiten su uso, exigiendo ciertas condiciones para su utilización, como un etiquetado que indique su uso, con el fin de ofrecer transparencia al electorado. La variación en los enfoques de la cuestión refleja la diversidad ideológica de estados como California, Minnesota, Texas, Washington y Florida (Rubio Núñez; Alvim; Monteiro, 2024).

Las normativas que se ocupan de las falsedades ultrarrealistas y otros medios de comunicación engañosos en las elecciones también varían en cuanto al periodo de prohibición o limitación, ya que algunas establecen un plazo previo a las elecciones para la prohibición (normalmente entre 60/120 días) y otras hacen que las restricciones sean permanentes (Norden; Narang; Protzmann, 2024).

En Minnesota y Texas, el uso de deepfakes para influir en las elecciones se considera delito penal cuando se producen o difunden en los 90 y 30, respectivamente, días anteriores a las elecciones, con sanciones que varían en función de la gravedad del acto. Washington cuenta con una normativa más completa que facilita el acceso de las víctimas a medidas cautelares u otras formas de reparación. La normativa obliga a *etiquetar* los contenidos manipulados y permite a los candidatos perjudicados demandar a los responsables de comunicaciones con contenidos “deepfake” o ultrafalsos, aunque los medios de comunicación están exentos de responsabilidad en algunas situaciones. Por último, Florida impone la obligación de etiquetar cualquier material generado por IA que cree una falsa apariencia de realidad con el fin de atacar a un candidato o influir en cuestiones electorales. El incumplimiento de estas normas puede dar lugar a sanciones penales (Rubio Núñez; Alvim; Monteiro, 2024). Otro ejemplo de iniciativa reguladora procede de Mississippi, estado que aprobó una legislación que prevé sanciones penales por la distribución, en el período de 90 días anterior a las elecciones, de contenidos digitales sin consentimiento con el fin de perjudicar a un candidato, impedir el ejercicio del voto o influir en las elecciones.

Como hemos visto, la manipulación de la información en contextos electorales no sólo ha servido para generar ventajas para los candidatos, sino también como método para alimentar el descrédito contra las instituciones electorales y favorecer la impugnación ilegítima de los resultados. En este sentido, reforzar la confianza y proteger a los

funcionarios electorales de la intimidación, el acoso y las amenazas es esencial para el desarrollo normal y pacífico de las elecciones. La utilización de los recursos de la IA para la producción y difusión generalizada y selectiva de contenidos sintéticos engañosos plantea aquí un verdadero desafío.

A principios de octubre de 2024, se presentaron una serie de proyectos de ley al gobernador de California. Aunque la iniciativa más esperada por los defensores de una regulación más exhaustiva fue vetada -la SB 1047 que estipulaba que las empresas tendrían que realizar pruebas de sus sistemas de IA antes de lanzarlos- se firmaron proyectos de ley que aumentan la transparencia y la responsabilidad en el uso de la inteligencia artificial en las elecciones (Lima-Strong, 2024). Los textos aprobados obligan a las plataformas digitales a retirar o etiquetar el material engañoso o manipulado digitalmente sobre las elecciones (AB 2655), a proporcionar transparencia en los contenidos utilizados en las elecciones que hayan sido producidos por IA (AB 2355). Además, se aprobó una ley que aumenta el plazo para prohibir la distribución de contenidos materialmente engañosos sobre candidatos por un periodo de 60 días antes de las elecciones a 120 días después (AB 2839).

En cuanto a la protección del propio proceso electoral, el estado de Kentucky debatió un proyecto de ley -que no fue aprobado- para penalizar la difusión de *deepfakes* que pudieran afectar al desarrollo de procesos administrativos, incluyendo, en este caso, la administración y los resultados de unas elecciones (KY House Bill n. 45). Los estados de Nueva Jersey (NJ House Bill n. 736) e Illinois (IL House Bill n. 4763) siguen debatiendo proyectos de ley para regular el uso de *deepfakes* que afecten a los procesos electorales (Norden; Narang; Protzmann, 2024).

La regulación del uso de *chatbots* en contextos electorales también ha sido objeto de debate tanto a nivel estatal como federal. Varios estados han considerado requisitos para el uso de esta funcionalidad, como la necesidad de identificación previa de que el usuario está interactuando con un sistema de inteligencia artificial (NY Assembly Bill n. 9103), la visualización de una advertencia de que el sistema puede ser inexacto o inapropiado (NY Assembly Bill n. 10103) y también el requisito de consentimiento afirmativo por parte del usuario (CA Assembly Bill n. 3211). Estos requisitos de transparencia y consentimiento previo también se han exigido en proyectos de ley que discuten -aún sin definir- el uso de voz sintética en llamadas automatizadas en el contexto de disputas electorales (Norden; Narang; Protzmann, 2024).

Algunos Estados también están estudiando las posibilidades de que los sistemas de IA ayuden a resolver viejos retos de sus sistemas electorales, como el problema que

supone la redistribución de distritos, blindando la distribución del electorado frente al *gerrymandering.* Otros están avanzando en proyectos que, aunque no están directamente relacionados con el proceso electoral, tienen la capacidad de producir efectos indirectos en las elecciones estadounidenses, como las propuestas que exigen la inclusión de marcas de agua en los contenidos generados por IA (AB-3211 California Digital Content Provenance Standards; OK House Bill n. 3453), así como la creación de sanciones contra *las deepfakes* por "uso ilegal" y medidas relacionadas con la protección de la privacidad de los usuarios (Norden; Narang; Protzmann, 2024).

Además del tratamiento normativo desarrollado por los estados, a finales de 2023 se publicó la Orden Ejecutiva sobre el Desarrollo y Uso Seguro y Confiable de la Inteligencia Artificial (Casa Blanca, 2023), que regula la explotación de las potenciales aplicaciones de los sistemas de IA y la gestión de los riesgos que acompañan a estas acciones innovadoras. Creada con el objetivo de equilibrar los aspectos positivos y negativos de la IA frente a los retos que han surgido con el rápido avance de las funcionalidades de los sistemas de IA, la Orden ofrece elementos que sirven de parámetro para orientar la comprensión de lo que puede entenderse como el uso seguro y fiable de las aplicaciones de IA emprendidas por la Administración Pública, sirviendo incluso de referencia para la acción reguladora internacional (Barbosa, 2023). Este documento presenta directrices objetivas para la acción de las entidades gubernamentales, en particular en lo que se refiere a: a) normas y reglas relativas a la seguridad en las aplicaciones que utilizan sistemas de IA (Sección. 4); b) promoción de la innovación y la competitividad entre *los actores* (Sección 5); c) respeto de los derechos, incluidos los de los trabajadores (Sección 6), civiles (Sección 7), consumidores y otros (Sección 8); d) protección de la privacidad (Sección. 9).

Aunque la gran mayoría de los debates están aún en construcción, y un número considerable de las iniciativas son todavía proyectos legislativos, la evolución de las discusiones en Estados Unidos, al tiempo que indica un cambio de actitud frente a los retos que plantea el uso de la IA en contextos electorales, también sugiere el advenimiento de un nuevo entorno normativo para futuras elecciones.

c. *Canadá*

En Canadá, la toma de decisiones automatizada está regulada desde 2019 con el fin de reducir los riesgos de error y discriminación. Este enfoque asegura una posición destacada a los requisitos de transparencia, incluyendo la obligación de informar

claramente de que la decisión procederá de un sistema automatizado, el deber de hacer público cualquier código fuente utilizado por la Administración Pública, así como la adopción de medidas cautelares dirigidas a la detección previa de sesgos involuntarios en los datos, el seguimiento de los resultados de estas decisiones y la garantía de la intervención humana y la recurribilidad de las decisiones (Rubio Núñez; Alvim; Monteiro, 2024).

En la dimensión electoral, en marzo de 2024 se presentó un proyecto de ley (C-65) que propone enmiendas a la Ley Electoral de Canadá -ya actualizada con la Ley de Modernización de las Elecciones (2018)- con el objetivo de aumentar la confianza y la participación en el proceso electoral. Este proyecto, de amplio alcance temático, incluye propuestas dirigidas a proteger la integridad del sistema electoral frente a amenazas tecnológicas, como el uso indebido de la inteligencia artificial (IA) y *las deepfakes* (Gobierno de Canadá, 2024). La IA, en particular, se menciona en el texto en un contexto de preocupación por la propagación de la desinformación y el riesgo de manipulación del proceso electoral.

d. *Europa*

A nivel europeo, se han identificado iniciativas tanto en la UE como en los propios países.

Unión Europea

En la Unión Europea, el Consejo Europeo aprobó en mayo de 2024 la Ley de Inteligencia Artificial (AI Act), basada en las recomendaciones de un Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial (AI HLEG) creado por la Comisión Europea. Su objetivo es regular el desarrollo, uso e impacto de la IA en diversos sectores, creando un marco normativo sólido y equilibrado que promueva la innovación tecnológica al tiempo que protege los derechos fundamentales.

La normativa se estructura a partir de un enfoque basado en el riesgo, clasificando los sistemas de IA en cuatro categorías:

1. **IA de riesgo inaceptable**: Se trata de sistemas que se consideran una amenaza para la seguridad, los derechos humanos y los valores fundamentales de la Unión Europea. Se consideran prohibidos los sistemas de IA que emplean manipulación cognitiva,

técnicas subliminales o engañosas, “scoring” (puntuación) social, explotación de vulnerabilidades como la edad o el estatus económico, vigilancia masiva, entre otros.

2. **IA de alto riesgo**: se trata de sistemas aplicados en sectores sensibles como la sanidad, las infraestructuras críticas, la educación y, en particular, los procesos democráticos y electorales. Estos sistemas están sujetos a estrictos requisitos de cumplimiento, que incluyen auditorías, transparencia, seguridad de los datos y vigilancia humana.
3. **IA de riesgo limitado**: Son aquellas que tienen pocas implicaciones para los derechos fundamentales y no requieren grandes restricciones, estando sujetas a obligaciones de transparencia más laxas para ayudar al usuario a tomar decisiones informadas. Algunos ejemplos son los chatbots sencillos o los sistemas de recomendación.
4. **IA de riesgo mínimo:** Se trata de sistemas que no plantean riesgos significativos y, por tanto, pueden funcionar sin regulación. La mayoría de los sistemas de IA en funcionamiento pertenecen a esta categoría.

A pesar de su carácter general, el documento contiene algunas disposiciones que influyen directamente en los procesos electorales, como las obligaciones específicas de transparencia impuestas a los sistemas que interactúan con personas físicas o que gestionan contenidos que suponen un riesgo de suplantación de identidad o engaño, utilizados actualmente de forma habitual en las campañas electorales para facilitar la interacción entre candidatos y votantes.

Además, la Ley de IA prohíbe los sistemas de IA capaces de promover influencias cognitivas manipuladoras, subliminales o engañosas en la formación de la voluntad de los votantes, ya que estas herramientas entrañan riesgos inaceptables bajo el prisma de las libertades individuales y la defensa de la democracia. Con esta medida, la ley impide la explotación de vulnerabilidades de determinados grupos sociales, prohibiendo así soluciones informáticas que promuevan la vigilancia masiva como forma de obtener datos que desencadenen la microsegmentación del votante.

La ley también regula el uso de sistemas de alto riesgo que puedan amenazar infraestructuras esenciales relacionadas con el proceso electoral, como el funcionamiento regular de los órganos electorales, los partidos políticos, las instituciones encargadas de la gestión del censo electoral o la expedición de los documentos necesarios para votar, entre otros. Todos los sistemas de IA de esta categoría deben garantizar: a) un modelo robusto de gobernanza de datos, manteniendo estándares de calidad y eliminando sesgos y discriminaciones; b) seguridad y supervisión humana en todos los ciclos; c) transparencia sobre su funcionamiento; d) registro en una base de datos comunitaria; y e) superación de

una prueba de conformidad, con la correspondiente certificación (Rubio Núñez; Alvim; Monteiro, 2024).

Incluso en relación con los sistemas que ofrecen un riesgo medio o bajo, que no presentan un peligro significativo -como *los chatbots* básicos-, la normativa también se aplica, exigiendo unas medidas mínimas de transparencia que permitan a los usuarios comprender su funcionamiento y sus principales atributos (Rubio Núñez; Alvim; Monteiro, 2024).

Alemania

Alemania ha desarrollado un marco jurídico muy completo que abarca la regulación de la inteligencia artificial y las tecnologías digitales. La lógica de este sistema normativo se basa en un estricto régimen jurídico de protección de datos personales, transparencia y rendición de cuentas. Este sistema regulador aumenta la posibilidad de que los sistemas de IA se utilicen de forma que se preserven los valores democráticos y la integridad electoral.

La base normativa central es el Reglamento General de Protección de Datos (RGPD), aplicado en 2018. Este reglamento es una de las piezas más completas de la legislación de protección de datos en el mundo, estableciendo estrictas normas de privacidad para todos los miembros de la Unión Europea. El GDPR influye profundamente en la forma en que los partidos políticos y los candidatos recopilan, gestionan y utilizan los datos personales, especialmente para la segmentación electoral, con importantes consecuencias para la aplicación de tecnologías como la IA en las campañas electorales (Sapada; Arif, 2024). Existen derechos a saber con qué fin se están utilizando sus datos, a tener acceso a sus datos y a que esos datos sean inutilizados. En el marco de esta legislación, se requiere el consentimiento expreso del usuario para que las organizaciones procesen datos privados (artículo 6).

Al mismo tiempo, la Ley alemana de Mejora del Cumplimiento de la Normativa en Medios Sociales (NetzDG), aprobada un año antes, impone a las plataformas digitales la obligación de retirar los contenidos claramente ilegales en un plazo de 24 horas a partir de la notificación de los usuarios interesados. También obliga a las empresas tecnológicas a elaborar informes de transparencia semestrales y establece un régimen de responsabilidad subjetiva, por el que los proveedores pasan a ser responsables cuando se compruebe que han incumplido de forma sistemática y reiterada los nuevos requisitos legales, especialmente a la hora de atender las quejas de los usuarios por contenidos ilegales. En

definitiva, la NetzDG pretende restablecer la salud del entorno informativo diseñando un modelo basado en la "obligación de retirar contenidos mediante la responsabilidad indirecta de supervisión (*Störerhaftung*)". (Eifert, op. cit., p. 164).

Reino Unido

En marzo de 2023, el Gobierno del Reino Unido publicó un documento titulado "A pro-innovation approach to AI regulation" (Un acercamiento en favor de la innovación a la regulación de la IA), también conocido como el "Libro Blanco del Reino Unido". Este *documento político* presentaba propuestas para implantar un marco regulador favorable a la innovación dirigido al uso de sistemas de IA en el Reino Unido (Gobierno británico, 2023).

Se previeron cinco principios transversales para guiar e informar el desarrollo y uso de sistemas en todos los sectores, sirviendo así de base para definir el enfoque regulador del Reino Unido: a) seguridad, protección y solidez; b) transparencia y “explicabilidad” adecuadas; c) equidad; d) responsabilidad y gobernanza; y e) impugnación y reparación.

Una vez finalizado el periodo de consulta, el Gobierno publicó una respuesta a los *comentarios* recibidos, contestando a las críticas de que era difícil extraer de este marco regulador una protección adecuada contra riesgos sistémicos como la desinformación y la interferencia en las elecciones.

El documento reconoce la necesidad de proteger la democracia contra las injerencias electorales mediadas por la IA, y se ha incluido un apartado específico sobre el tema, titulado "Proteger la democracia de las injerencias electorales". Uno de los puntos centrales es el fortalecimiento del Grupo de Trabajo para la Defensa de la Democracia, cuyo objetivo es involucrar a expertos de diversas áreas del gobierno para mitigar las amenazas, especialmente la interferencia extranjera en los procesos electorales. Este grupo de trabajo demuestra la intención del Reino Unido de desarrollar estrategias de prevención sólidas, centradas en la cooperación entre distintos organismos y en el uso de conocimientos técnicos para hacer frente a los nuevos retos que plantea la IA generativa.

Otro elemento clave del enfoque normativo del Reino Unido es la revisión de las leyes electorales vigentes, que ha dado lugar a la introducción de un nuevo régimen de "huella digital" en la Ley Electoral de 2022. Esta medida exige que los materiales digitales de campaña dirigidos al electorado incluyan información clara sobre los responsables de crear y distribuir estos contenidos, como su nombre y dirección. La introducción de esta obligación aumenta la transparencia y permite a los votantes identificar fácilmente a los autores de los materiales políticos, incluidos los generados por IA. De este modo, el

Gobierno pretende dificultar el uso de herramientas de IA para difundir desinformación durante el periodo electoral, promoviendo una mayor responsabilidad por parte de quienes participan en la producción de contenidos electorales.

Por último, el Gobierno británico ha propuesto poner marcas de agua a los contenidos relacionados con las elecciones como una estrategia más de transparencia. Esta medida pretende garantizar que los votantes tengan una mayor confianza en los contenidos a los que acceden en línea, permitiéndoles identificar mejor el material auténtico. En conjunto, estas estrategias reflejan un esfuerzo coordinado para preservar la integridad electoral frente al creciente uso de la IA, evitando la manipulación y la influencia indebida en el proceso democrático (Soon; Quek, 2024).

Irlanda

En vísperas de las elecciones al Parlamento Europeo de abril de 2024, la Comisión Electoral Independiente de Irlanda publicó un Marco sobre información del proceso electoral en línea, publicidad política y contenido engañoso de la IA. El documento no tiene carácter vinculante, sino voluntario, y sirve de guía indicativa de buenas prácticas en este ámbito. Con un enfoque basado en los riesgos, el estatuto se dirige tanto a las plataformas en línea como a los motores de búsqueda, los partidos políticos registrados y los candidatos. A la hora de redactar la normativa se ha tenido en cuenta la necesidad de garantizar un equilibrio razonable entre el ejercicio de los derechos fundamentales de libertad de expresión y opinión, y de participación en los asuntos públicos, con la protección del entorno democrático y la integridad de las elecciones.

Según los términos del estatuto, la publicidad política en línea debe utilizarse prestando atención a los principios de transparencia y respeto de la integridad electoral, y debe indicar de forma clara, visible y eficaz que se refiere a contenidos electorales. También es necesario que los actores relevantes del proceso electoral actúen para proteger las elecciones de la desinformación en el entorno digital, previendo específicamente la creación de un mecanismo de denuncia de incidentes. En lo que respecta específicamente al uso indebido de sistemas de inteligencia artificial en los procesos electorales, el estatuto establece que los actores relevantes en el proceso electoral deben promover herramientas para mitigar los riesgos relacionados con la producción de contenidos engañosos, incluidos los deepfakes. Además, es necesario desarrollar mecanismos para etiquetar adecuadamente las imágenes, audios y vídeos producidos sintéticamente que puedan resultar confusos o engañosos (Coimisiún Toghcháin, 2024).

e. *Otras experiencias*

India

En la India, en 2024 los partidos políticos invirtieron más de 50 millones de dólares en contenidos producidos por inteligencia artificial, que incluían *deepfakes* de figuras políticas fallecidas (Dutt, 2024) y manipulación de imágenes de celebridades. Aunque el organismo electoral indio (*Election Commission India* - ECI) cuenta con un marco normativo orientado a las tecnologías de la información (la *Ley de Tecnologías de la Información* - IT Act) que, por regla general, regula las plataformas de Internet, le ha resultado difícil hacer frente al uso irregular de las redes sociales y los servicios de mensajería en las elecciones, especialmente debido a que el código de conducta que rige el comportamiento en las plataformas sociales no es vinculante (Gupta; Mathews, 2024).

Ante los reiterados casos de irregularidades, la ECI envió una comunicación a todos los partidos políticos en la que pedía un uso ético y responsable de las plataformas de medios sociales y destacaba, entre varias disposiciones normativas, el artículo 66D de la Ley de Tecnologías de la Información, que prevé el castigo de las personas que utilicen dispositivos de comunicación o informáticos con intención maliciosa, induciendo a error de identidad o engaño (Indian Express, 2024). Sin embargo, dada la falta de mecanismos legales más eficaces, las consecuencias de las infracciones no suelen ser graves (Gupta; Mathews, 2024).

India carece actualmente de un marco normativo específico para la IA. Sin embargo, dado el creciente número de casos relacionados con el uso indebido de soluciones inteligentes en procesos electorales, incluido un episodio en el que la herramienta Gemini (desarrollada por Google) presentó una respuesta que sugería que algunos expertos entendían que el primer ministro indio había aplicado políticas fascistas (Dhillon, 2024), las demandas de regulación han ido en aumento (Gupta; Mathews, 2024). En julio, se informó que el Ministerio de Electrónica y Tecnología de la Información está elaborando una legislación centrada en la inteligencia artificial, que exigirá el etiquetado de los contenidos producidos por IA. También está estudiando parámetros legales para que los grandes modelos lingüísticos (LLM) se entrenen en lenguas indias y con contenidos específicos del contexto local (Barlk, 2024).

Corea del Sur

En Corea del *Sur*, en enero de 2024 entró en vigor una enmienda a *la Ley de Elecciones de Funcionarios Públicos* que prohíbe el uso de deepfakes producidos por IA en los 90 días anteriores al día de las elecciones. Como resultado, el artículo 82(8) de la ley establece ahora que: "[n]adie puede producir, editar, distribuir, mostrar o publicar vídeos *deepfake* con fines de campaña electoral desde 90 días antes del día de las elecciones hasta el día de las elecciones" (Comisión Electoral Nacional de la República de Corea, 2024). La ley prevé una pena de hasta siete años de prisión o una multa de unos 35.000 dólares (Soon; Quek, 2024). Por otra parte, en las elecciones coreanas está permitido el uso de herramientas ingeniosas para promover la participación política mediante la producción de eslóganes de campaña, jingles y discursos (Chakravarti, 2024).

Singapur

El enfoque de Singapur sobre el uso de la IA en las elecciones se caracteriza por centrarse en la transparencia, la rendición de cuentas y la mitigación de las amenazas de desinformación e injerencia extranjera. Aunque el país aún no cuenta con una normativa dirigida exclusivamente a la IA en las elecciones, Singapur adopta un marco regulador que abarca tres ámbitos principales: desinformación, propaganda política e injerencia extranjera (Soon; Quek, 2024). Documentos como la Ley de Protección contra Falsedades y Manipulación en Línea *(Protection from Online Falsehoods and Manipulation* Act, POFMA) y la Ley de Contramedidas contra la Interferencia Extranjera (*Foreign Interference Countermeasures Act*, FICA) pretenden combatir la difusión de información falsa y las influencias externas que puedan poner en peligro la integridad de las elecciones.

Además, Singapur aplica estrictos requisitos de transparencia en la publicidad política, especialmente en el contexto en línea. La Ley de *Elecciones Parlamentarias* y la *Ley de Elecciones Presidenciales* establecen requisitos de divulgación para los anuncios electorales, incluida la identificación clara de quién financia y autoriza el contenido. Estas medidas ayudan a garantizar que el público pueda verificar la fuente de la información, minimizando el impacto de las campañas de desinformación o manipulación, potencialmente reforzadas con el uso de IA (Soon; Quek, 2024).

En septiembre de 2024, el Ministerio de Desarrollo Digital e Información (MDDI) presentó un proyecto de Ley Electoral a través del cual busca incluir nuevas medidas de

protección más efectivas contra la manipulación digital de contenidos en procesos electorales, lo que incluye el uso de sistemas de inteligencia artificial para producir *deepfakes.* El proyecto de ley propone prohibir la publicación de contenidos publicitarios electorales generados o manipulados digitalmente que muestren de forma realista a un candidato diciendo o haciendo algo que no ha sucedido. También prevé la posibilidad de emitir instrucciones correctivas para la retirada de contenidos ofensivos o inhabilitar el acceso de los usuarios a dichos contenidos en el país, estableciéndose sanciones de multa, prisión o ambas por el incumplimiento de estas medidas (Gobierno de Singapur, 2024). Los candidatos que publiquen contenidos falsos o engañosos se exponen a multas o incluso a la pérdida de sus escaños (Iau, 2024).

6. Enfoque jurisdiccional

Las decisiones judiciales sobre el uso de la IA en las elecciones son aún escasas en los tribunales electorales, ya sea por la ausencia o la juventud de leyes específicas, según los casos. Por ello, sigue existiendo una gran incertidumbre sobre cómo interpretar las escasas disposiciones legales que van apareciendo poco a poco.

En agosto de 2024, la Sala Especializada *del Tribunal Electoral del Poder Judicial de la Federación* de México analizó un anuncio publicitario basado en la imagen de un niño creada sintéticamente por un partido político en un contexto electoral. En su primer encuentro con el tema, el Tribunal dictaminó que el uso de este tipo de imagen podría poner en peligro el interés superior del niño, en contra de la Constitución mexicana. Según la sentencia, esta forma de propaganda caracteriza la instrumentalización de la infancia con fines políticos, lo que implica una violación de los derechos de niños, niñas y adolescentes. La utilización de imágenes infantiles en procesos electorales, por tanto, debe ir acompañada de una lógica superior de cuidado y protección. La Sala Especializada del Tribunal concluyó que la utilización de la imagen de un menor mediante el uso de tecnología de IA por parte de una campaña electoral supera los límites de la utilización de propaganda, ya que se trata de una simulación que pretende eludir la legislación nacional (SRE-PSC-369/2024). Sin embargo, la Sala Superior del TEPJF revocó, por mayoría de votos, la referida sentencia, considerando que la imagen en sí misma no expone a peligro potencial los derechos de la niñez. En el SUP-REC-893/2024 se ha decidido que se deben considerar las circunstancias de cada caso, y que el uso de la representación creada con IA no corresponde a utilizan la imagen de un menor de edad.

Al analizar la propaganda electoral con el uso de *deepfakes*, en el marco de la reciente reglamentación del TSE de Brasil (Resolución 23.610, actualizada en 2024), el Tribunal Regional Electoral de São Paulo, en Brasil, sostuvo que, para caracterizar una irregularidad, no basta la creación o manipulación de contenido con recursos sintéticos, sino que es necesario verificar si el uso de estos instrumentos produjo propaganda con verosimilitud y potencial efectivo de daño (REI nº 060005354). El caso se refería a un vídeo en el que el rostro de un candidato a la alcaldía de São Paulo se presentaba de forma ultrarrealista, sustituyendo al del personaje "Ken" de la película "Barbie". El Tribunal dictaminó que el contenido era legal, dada la baja calidad del montaje. Estableció así la percepción de que la ilegalidad depende de la "mínima posibilidad" de convencer al votante.

A su vez, el Tribunal Regional Electoral de Minas Gerais, también en Brasil, impuso una multa a un candidato que utilizó en su campaña la imagen de su difunto abuelo, que había sido alcalde durante cuatro mandatos diferentes. Para el Tribunal, la mera señalización de la naturaleza del contenido sintético no excluía la ilegalidad del anuncio, dada la violación expresa de la legislación electoral (REI 060080847). En otra decisión, el Tribunal sostuvo que la difusión de contenidos manipulados digitalmente con la intención de difamar a los candidatos constituye propaganda negativa irregular y justifica la concesión de una orden judicial para que se faciliten los datos que identifiquen a los responsables, con miras a proteger la integridad del proceso electoral (REI 060061190).

En Estados Unidos, en octubre de 2024, parte de una nueva ley promulgada por el Estado de California hace menos de un mes, que permitía a cualquiera demandar por daños y perjuicios derivados de *deepfakes* electorales, fue suspendida por un juez federal. Según el magistrado, la ley parece violar la Primera Enmienda de la Constitución, ya que "sofoca inconstitucionalmente el intercambio libre y sin trabas de ideas (Healey, 2024).

7. Clasificación de los resultados

Teniendo en cuenta la metodología expuesta en el capítulo 2 de este informe, las normas reglamentarias encontradas se clasifican ahora desde diez perspectivas diferentes.

En términos de **amplitud**, encontramos regulaciones que dan a la IA un enfoque *sistemático*, como la Ley de IA de la Unión Europea, que, si bien no trata la materia electoral de manera restringida, tiene efectos en la dinámica de organización de las elecciones. Por otro lado, también se identificaron casos en los que la informática inteligente recibe (o tiende

a recibir) un tratamiento integral dentro del *sistema electoral*, siendo esta la dirección adoptada por la Resolución 23.732/2024 del TSE de Brasil, así como el proyecto de reforma a la Ley Electoral de Canadá, casos emblemáticos de un enfoque *microsistemático*. El tratamiento *puntual*, sin embargo, apareció con más frecuencia dentro de la muestra, sobre todo en leyes concisas y específicas aprobadas, por ejemplo, en California (AB 2355, AB 2655 y AB 2839), que impusieron obligaciones específicas a las plataformas digitales en relación con el uso indebido de sistemas de IA en contextos electorales, además de ampliar el periodo en el que se prohíbe la difusión de material engañoso. Del mismo modo, se encontraron modificaciones específicas en Corea del Sur, en una disposición que prohíbe la explotación electoral de *deepfakes*.

En cuanto al **alcance de la intervención legal,** no se han identificado enmiendas *constitucionales* que regulen la cuestión, lo que puede explicarse tanto por el hecho de que las regulaciones electorales, por regla general, residen en normas infra constitucionales como por el hecho de que, también por regla general, las enmiendas constitucionales implican un procedimiento mucho más estricto para su aprobación. Sin embargo, se han producido importantes avances normativos a nivel de *la UE*, con la Ley Europea de IA, y también a nivel legal, con la promulgación de normas que elevan el nivel de protección ofrecido frente a los riesgos de los sistemas de IA, como las diversas leyes estatales estadounidenses que regulan el uso de *deepfakes* en las elecciones. También ha habido al menos una iniciativa normativa directamente derivada de un órgano de Justicia Electoral: el modelo brasileño, en el que las resoluciones, aunque son actos normativos secundarios, tienen el mismo *estatus* que las leyes formales.

En cuanto **a la premisa de la matriz reguladora**, hubo tanto *enfoques basados en el riesgo*, como la Ley de IA y el Reglamento General de Protección de Datos alemán (GDPR); como *híbridos*, como el proyecto de ley brasileño para regular el uso de la IA, que se centra tanto en preservar los derechos como en comprender los riesgos que ofrecen los sistemas de IA, calibrando con mayor rigor los modelos que conllevan mayores riesgos.

En cuanto al ámbito de aplicación de las normas analizadas, predominan las que establecen un *deber de diligencia impuesto a las plataformas* y la *responsabilidad de los actores políticos*, como se observa en el caso de la ley india sobre tecnologías de la información y la legislación surcoreana, que establece castigos en caso de producción y difusión de contenidos malintencionados (en este último caso, con posibilidad de penas de prisión). También encontramos *normas de protección de datos* que tienen un impacto considerable en los procesos electorales, como las leyes generales de protección de datos de Alemania y Brasil. También encontramos normas que responsabilizan a las plataformas

del incumplimiento de órdenes judiciales, como la Resolución 23.610 de Brasil y el reciente proyecto de ley de Singapur.

Analizando **los destinatarios de las normas sancionadoras**, observamos que la mayoría de las regulaciones se dirigen a *candidatos y entidades partidistas* y *a productores de contenidos y personas politizadas en general* (es decir, responsables de elaborar/manipular y difundir contenidos irregulares utilizando recursos de IA), a ejemplo del estatuto da Irlanda y la Resolución brasileña. También identificamos normativas dirigidas a productores*, desarrolladores y proveedores de sistemas de inteligencia artificial,* especialmente normativas basadas en riesgos como la Ley de IA.

En **cuanto a la naturaleza de las sanciones** previstas, algunas experiencias normativas incluyen *la retirada de contenidos*, como el proyecto de ley de Singapur, el NetzDG y la Resolución brasileña. También se identificaron *multas* económicas en la GDPR y la NetzDG alemanas, la Ley de IA y la Resolución brasileña, así como la posibilidad de *penas de prisión* en disposiciones de la legislación surcoreana y el Proyecto de Ley de Singapur. También existen normas legales en las que la consecuencia del uso indebido de la IA en las elecciones se castiga con la *pérdida del mandato*Proyecto de Ley de Singapur) - y, además, con la *inelegibilidad* de la persona implicada (Resolución brasileña). Cabe destacar que la legislación brasileña también prevé la *suspensión de los servicios de aplicaciones de Internet en* caso de incumplimiento, así como la *prohibición o suspensión* de *perfiles* y grupos o canales de medios sociales dedicados a la desinformación. Vino desde ahí la suspensión temporal del funcionamiento de la plataforma X en el país, como medida de *ultima ratio* tras la negativa sistemática de cumplimiento a órdenes de bloqueo de cuentas de importantes actores difusores de desinformación contra la integridad electoral.

En cuanto **a los niveles de actuación legislativa**, la Resolución brasileña enumera una serie de medidas dirigidas a las plataformas, con el objetivo de frenar la difusión de contenidos sintéticos irregulares en los procesos electorales. Se han establecido diversas obligaciones, entre ellas la necesidad de *estar autorizado para prestar servicios político-electorales*, así como medidas que inciden en el *modelo de negocio* (como elaborar y aplicar condiciones de uso y políticas de contenidos compatibles con los objetivos de la resolución, implementar canales de denuncia y notificación, transparencia de resultados, etc). Cabe destacar que estas exigencias han llevado a algunas plataformas, como Google, a anunciar que no permitirán la difusión de contenidos político-electorales de pago (Agência Brasil, 2024).

En una línea similar, en Europa la Ley de IA estableció diversas medidas obligatorias para el funcionamiento de los sistemas inteligentes, con mayores niveles de rigor para aquellos que ofrecen mayores riesgos sistémicos, lo que incluye obligaciones de prudencia en relación con la *programación algorítmica*. *El control de comportamientos* inadecuados fue un enfoque predominante en los documentos estudiados, con prohibiciones sobre el uso de agentes robóticos y perfiles de uso falsos, así como restricciones sobre el uso de herramientas de activación masiva en Brasil. También encontramos una recurrencia de una postura rígida *en el control de contenidos*, con la mayoría de los instrumentos estableciendo parámetros de legalidad para el contenido de la publicidad. Un ejemplo de ello se observa en el tratamiento de la cuestión por parte de los distintos Estados americanos estudiados, que prohíben los contenidos falsos mediante la tecnología *deepfake*.

En cuanto a los **bienes jurídicos protegidos por las normas de limitación de contenidos,** las medidas suelen proteger simultáneamente diversos bienes jurídicos deseables en el proceso electoral, como *la libertad de sufragio*, la *igualdad de oportunidades*, el *honor y la dignidad de los candidatos* y la *imagen y confianza en las instituciones electorales*. Aunque no se indique explícitamente, las intenciones pueden entenderse a partir de normas que señalan la nocividad de los contenidos engañosos que causan vergüenza cognitiva o dificultan el ejercicio consciente de la ciudadanía.

La Ley General de Protección de Datos alemana es una de las normativas que mejor demuestra un enfoque dirigido a *proteger el derecho a la intimidad de los usuarios.* En cuanto a *la protección de grupos vulnerables o minoritarios*, fue posible identificar restricciones al uso de sistemas de IA basadas en la *puntuación social*, las condiciones económicas u otros análisis de características personales que implican discriminación. Un ejemplo relevante es la prohibición de prácticas de IA en la legislación comunitaria, especialmente cuando prohíbe la comercialización de servicios que utilicen IA que impongan un trato desfavorable a personas o segmentos sociales de forma injustificada y desproporcionada (Art. 5, 1, c de la Ley de IA de la Unión Europea). Por regla general, todas las normas estudiadas se dirigen, aunque de forma indirecta, a garantizar el *carácter pacífico de las elecciones y la estabilidad democrática y la paz social*, aunque las normas brasileñas que combaten la violencia, la incitación al odio, el extremismo y la radicalización lo hacen de forma más visible.

En cuanto al grado de cobertura de los riesgos cartografiados, encontramos un enfoque predominante en los riesgos derivados de la *desinformación electoral* y su *impacto en los derechos humanos*, lo que a veces da lugar a que la IA sea tratada sólo

como parte de los esfuerzos contra los desórdenes informativos en el contexto de las elecciones. En este sentido, por ejemplo, el caso de Corea del Sur. La preocupación por el aumento de la violencia *política, la discriminación y el acoso* se observa en algunos esfuerzos normativos que abarcan también la prevención de conflictos, como la resolución brasileña, que prevé un tratamiento específico en relación con las conductas que caracterizan los actos de violencia política y discriminación. Por último, el control dirigido al *uso irregular de los datos personales* se verificó ampliamente en las normativas estudiadas, como se observa en las leyes generales de datos personales alemana y brasileña, así como en la legislación de la Comunidad Europea.

8. Conclusión y catálogo de recomendaciones

La incapacidad para adaptarse a las transiciones tecnológicas pone en tela de juicio la capacidad de los órganos de administración electoral para responder adecuadamente a la difusión de contenidos nocivos que circulan intensamente en los medios digitales. En este sentido, la capacitación técnica de los equipos internos puede verse como un prerrequisito para la materialización de respuestas ágiles y efectivas que eviten o mitiguen los daños asociados a escenarios de crisis.

Por lo tanto, es esencial que las instituciones electorales establezcan alianzas con entidades especializadas en tecnología y protección de datos, con el fin de comprender mejor las herramientas utilizadas para difundir narrativas perjudiciales y desarrollar estrategias adecuadas para hacerles frente (Goltzman; Lopes, 2024). Al fin y al cabo, la brecha de conocimiento en este ámbito concreto "no es meramente superficial, sino fundamental para la aplicación efectiva de la justicia en un contexto tecnológicamente saturado" (Tavares, 2024).

El creciente uso de la inteligencia artificial en los procesos electorales, especialmente a escala nacional, demanda un enfoque regulatorio robusto, oportuno[20] y técnicamente adecuado que tome en cuenta tanto la mitigación de riesgos y la creación de mecanismos para desalentar prácticas nocivas como, por otro lado, la maximización de los beneficios que potencialmente ofrece esta tecnología. A través de este lente, los organismos electorales deben seguir de cerca los movimientos legislativos, con miras a asegurar que,

[20] A pesar de todas las dificultades, es vital darse cuenta de que, dadas las cuestiones discutidas anteriormente, la inercia regulatoria también debe entenderse como un enorme riesgo en sí mismo (Sapada; Arif, 2024), ya que la ausencia de reglas, condiciones y límites expone a las competencias electorales a una nueva colección de disfunciones tecnológicas muy concretas y significativas.

en la medida de lo posible, se presenten agendas relacionadas con la protección de la mecánica electoral.

Además, corresponde a los órganos de justicia electoral adoptar estrategias creativas e integrales para garantizar que la computación inteligente, en el ámbito de sus competencias, sea utilizada de forma ética y de acuerdo con los principios democráticos, teniendo en cuenta la advertencia de que "posponer el enfrentamiento directo de esta cuestión aumentará el nivel de dificultad para contener y corregir los efectos nocivos ya causados" (Tavares, 2022). Además, por el momento conviene admitir, sin más, que "no es posible afrontar los males de la IA sin la IA" (Rubio Núñez; Alvim; Monteiro, 2024).

Buscando sistematizar y ampliar un camino inicialmente pavimentado por una amplia gama de autores (Assibong et al, 2019; Chennupati, 2024; Juneja, 2024; Muñoz, 2024; Ogwuche; Onah, 2023; Panditjaratne; Giansiracusa, 2023; Rubio Núñez; Alvim; Monteiro, 2024; Sook; Quek, 2024; Tuset Varela, 2024; Yazbek, 2024; Yu, 2024), presentamos una lista de recomendaciones para la aplicación democrática de la inteligencia artificial en las campañas y procesos electorales:

1. **Establecimiento de normas específicas para el uso de la IA**: La regulación debe prever un marco específico que aborde las particularidades de la IA en el contexto de la contienda por los votos, centrándose en garantizar que su uso no comprometa la integridad del proceso electoral. Deben establecerse normas claras para evitar la difusión de desinformación, la ruptura de la autenticidad de los diálogos públicos con la participación de *bots* y otras formas de interferencia indebida. La divulgación obligatoria del uso de la IA, incluido el etiquetado de IAGen los documentos de comunicación, y la divulgación pública de los recursos de minería de datos y segmentación de votantes son pasos cruciales en este sentido.
2. **Transparencia y rendición de cuentas**: Debe exigirse un alto grado de transparencia en relación con el uso de la IA en campañas y procesos de administración electoral. Esto incluye la obligación de hacer público el uso de algoritmos para la segmentación de votantes o la generación de contenidos, así como los criterios utilizados por estos sistemas. La rendición de cuentas es esencial para garantizar que las prácticas adoptadas respetan los derechos de los votantes y el principio de igualdad de acceso a la información.
3. **Ampliar la supervisión reglamentaria**: Ampliar el ámbito reglamentario para incluir explícitamente la IA es fundamental. El actual régimen jurídico electoral debe adaptarse para contemplar los impactos de la IA en todas las fases del proceso electoral,

desde la campaña hasta el recuento de votos, promoviendo una supervisión continua y eficaz. Una parte importante de estos esfuerzos pasa por establecer un marco de regulación de datos capaz de salvaguardar a los interesados, garantizar un acceso lícito y justo e impedir el uso indebido.

4. **Cooperación con el sector tecnológico**: Debe ampliarse la interacción con plataformas digitales y empresas líderes en el desarrollo de IA. Un diálogo continuo entre los organismos electorales y el sector privado permitirá una mejor comprensión de los desafíos tecnológicos y proporcionará insumos para la creación de regulaciones que sean técnicamente viables y adecuadas al contexto electoral. Eventualmente, estos acercamientos podrían resultar en acuerdos específicos para adaptar los productos a las necesidades sociales. Además, es importante exigir a los proveedores de medios sociales que adapten sus términos y condiciones al contexto, los actualicen y los apliquen de forma clara, coherente y con impacto. Las medidas para aumentar las barreras de registro, eliminar los bots y reducir la alteración de la autenticidad de los diálogos virtuales son esenciales desde esta perspectiva. Lo mismo cabe decir de la inserción de elementos de fricción para dificultar el acceso, la compartición, la viralización y el consumo involuntario de contenidos nocivos.

5. **Participación de la sociedad civil**: La participación de organizaciones de la sociedad civil, expertos en tecnología y grupos de derechos políticos es esencial para legitimar el proceso de regulación. Crear mecanismos institucionales para escuchar y considerar las preocupaciones y sugerencias de estos actores puede reforzar la confianza pública en las elecciones y garantizar que la regulación sea sensible a las demandas sociales. También es importante construir una agenda orientada a fomentar la innovación. Finalmente, los órganos de administración electoral deben buscar acuerdos con actores estratégicos que puedan satisfacer parte de sus necesidades estratégicas, con el fin de ampliar sus capacidades institucionales.

6. **Seguimiento y evaluación continua**: La naturaleza dinámica de las tecnologías de IA requiere un enfoque regulatorio que permita la revisión y actualización periódica de las normas aplicables. La creación de comités consultivos formados por expertos en IA, ciencia de datos, comunicación política y derecho digital, así como el desarrollo de investigaciones cualitativas con profesionales de estas áreas, pueden garantizar que la regulación se mantenga actualizada ante las innovaciones tecnológicas y los nuevos riesgos emergentes.

7. **Identificar las aplicaciones beneficiosas de la IA**: Además de la regulación destinada a mitigar los riesgos, es importante identificar y fomentar el uso de la IA para

mejorar la seguridad, la eficiencia, la fiabilidad y la accesibilidad de los procesos electorales. Sin embargo, la inteligencia artificial debe considerarse como un medio para alcanzar objetivos fundamentales, y no como un fin en sí misma. En este sentido, las organizaciones electorales deben pensar en cómo aplicar la inteligencia artificial para alcanzar los objetivos contenidos en su planificación estratégica, y no en cómo adaptar su planificación estratégica para dar cabida de algún modo a algunas soluciones de IA.

8. **Responsabilidad de plataformas y usuarios**: La norma reguladora debe garantizar la atribución de responsabilidad tanto a los desarrolladores de tecnologías de IA como a los candidatos y partidos políticos que se benefician de sus aplicaciones. Deben existir disposiciones claras para exigir responsabilidades a quienes permitan o utilicen la IA de forma que se ponga en peligro la legitimidad del proceso electoral, mediante sanciones proporcionadas y efectivas, evitando, en la medida de lo posible, la imposición de sanciones basadas en prohibiciones genéricas, con cláusulas abiertas que generen inseguridad jurídica como consecuencia de un alto grado de abstracción.

9. **Sanciones y reparto de responsabilidades**: La adopción de un régimen de sanciones claro y proporcionado es crucial para inhibir el uso indebido de la IA. El reglamento debe prever no solo sanciones para los candidatos y partidos que hagan un uso inadecuado de la computación inteligente, sino también la rendición de cuentas de las plataformas digitales y los proveedores de tecnología que faciliten estas prácticas[21]. El reparto de responsabilidades entre todos los actores implicados contribuirá a la eficacia del reglamento y a la protección del proceso electoral.

10. **Fomentar la educación mediática y la educación informativa**: Invertir tiempo y energía en proyectos pedagógicos puede ayudar a desarrollar la capacidad de resistencia del público frente a la desinformación. La educación mediática desarrolla la capacidad crítica ante los contenidos, mitigando el exceso de credulidad que facilita la interiorización de falsas narrativas. Por otro lado, anima a los usuarios a utilizar de forma segura y responsable las herramientas tecnológicas, desde internet a las redes sociales, pasando por la inteligencia artificial. La educación informativa, por su parte, refuerza la evaluación de la credibilidad de la información, capacitando a la audiencia para valorar correctamente la relevancia de los discursos, detectando las falacias argumentativas y separando las fuentes válidas de las inválidas, así como las afirmaciones de hecho de las meras opiniones.

[21] Al fin y al cabo, si está "[...] claro que la IA es utilizada tanto por los candidatos y las campañas como -a veces incluso con más intensidad- por los votantes y en diferentes formatos mediáticos (imagen, vídeo y audio), [...] las medidas reguladoras o las políticas públicas sobre el tema deben tener en cuenta los diferentes públicos" (Data Privacy Brasil; Alafialab, 2024).

10. **Considere el valor de la educación algorítmica y la educación para la inteligencia emocional:** La educación algorítmica empodera a los usuarios al proporcionarles una comprensión básica de cómo funcionan la inteligencia artificial y las plataformas de medios sociales, haciendo hincapié en los impactos sociales de la programación. Del mismo modo, la educación emocional puede contribuir a una agenda de transformación positiva, haciendo que los votantes sean menos susceptibles a las falsas narrativas y al chantaje argumentativo mediante la concienciación de la existencia de sesgos, disonancia cognitiva, fallos de procesamiento lógico derivados del pensamiento intuitivo y otras debilidades del aparato sensorial.

11. **Garantizar que la incorporación de tecnologías sensibles vaya precedida de campañas estratégicas de legitimación:** La fe pública en la IA y su aceptación son cruciales para su uso eficaz por parte de los organismos de administración electoral. Al no tener suficientes conocimientos sobre la tecnología, algunas personas pueden mostrarse desconfiadas o recelosas, lo que tiende a elevar el cuadro general de sospecha. Para confiar en la IA y utilizarla en las elecciones, la gente debe comprender sus ventajas, riesgos y limitaciones (Chennupati, 2024).

12. **Establecer políticas internas para garantizar el uso responsable de la IA:** Los organismos electorales deben estipular principios y directrices internas para garantizar el uso seguro y responsable de las herramientas inteligentes. Estas normas deben garantizar, entre otras cosas, la transparencia, la “explicabilidad” y los mecanismos de auditoría, así como prever protocolos de supervisión y garantizar la participación humana en todos los ciclos de inteligencia artificial. Las normas de revisión periódica, adaptabilidad y corrección de errores son indispensables. La adopción efectiva de soluciones de IA, sin embargo, debe ir precedida de estudios internos que consideren un equilibrio entre los riesgos implicados y los posibles beneficios, al tiempo que garanticen la debida atención a la proporcionalidad en términos de estructura, escala y volumen de operaciones.

13. **Alentar a los candidatos y partidos políticos a adherirse ampliamente a pactos éticos o códigos de conducta:** Aunque no tienen un peso imponente o valor contundente, los pactos éticos y códigos de conducta pueden arrojar resultados positivos, como efecto de un compromiso público asumido por las agrupaciones y actores electorales, especialmente en escenarios de desierto normativo.

14. **Activar alianzas estratégicas para una respuesta en red:** Dado el carácter global de la tecnología y la rápida exportación de estrategias de desinformación digital en red, las nuevas patologías de la comunicación política representan un horizonte común de desafíos para las organizaciones electorales. El diálogo y el intercambio de conocimientos

entre organismos de distintos países, así como la formación o el fomento de grupos de investigación académica, pueden marcar la diferencia, ya que aprender de experiencias pioneras puede evitar errores, eliminar vulnerabilidades y cualificar el trabajo de las instituciones.

9. Referencias bibliográficas

ABRANCHES, S. **O tempo dos governantes incidental**. São Paulo: Cia das Letras, 2020.

AGÊNCIA BRASIL. Google no permitirá anuncios políticos en las elecciones de octubre. **Agência Brasil**, 24 de abril de 2024. Disponible en: [https://agenciabrasil.ebc.com.br/justica/noticia/2024-04/google-nao-permitira-anuncios-de-politicos-nas-eleicoes-de-outubro]. Consultado: 21 de octubre de 2024.

AKBAR, P.; LOILATU, M.; PRIBADI, U.; SUDIAR, S. Implementation of Artificial Intelligence by the General Elections Comission in Creating a Credible Voter List. **ICONPO X**, n. 717, 2021, pp. 1-7.

ALMEIDA, P. G. R. de; SANTOS, C. D. do; FARIAS, J. S. Regulación de la Inteligencia Artificial: un marco para la gobernanza. **Ethics and Information Technology**, abril de 2021, pp. 505-525.

ALVIM, F. F. **Abuso de poder nas competições eleitorais**. 2. ed. Belo Horizonte: Fórum, 2024.

ARAMBURÚ MONCADA, L. G.; LÓPEZ REDONDO, I.; LÓPEZ HIDALGO, A. La inteligencia artificial en RTVE al servicio de la España vacía. Cobertura informativa con redacción automatizada para las elecciones municipales de 2023. **Revista Latina de Comunicación Social**, n. 81, 2023, pp. 1-16.

ARNOLD, R. Five principles for using technology to support election access and inclusion. **International Foundation For Electoral Systems**, octubre de 2023. Disponible en: [https://www.ifes.org/learning-series-disability-inclusive-election-technology]. Consultado: 23.10.2024.

ASSIBONG, P. A.; WOGU, I. A. P.; SHOLARIN, M. A.; MISRA, S.; DAMASEVIČIUS, R.; SHARMA, N. The Politics of Artificial Intelligence Behaviour and Human Rights Violation Issues in the 2016 US Presidential Elections: An Appraisal. En: SHARMA, N.; CHAKRABARTI, A.; BALAS, V. E. (Eds.). **Gestión de datos, análisis e innovación**. Proceedings of ICDMAI, vol. 2. Nueva York: Springer, 2019, p. 295-310.

BAHRI, P. R.; ASMARA, H. M. G.; HUM, M.; RISNAIN, M. Artificial Intelligence (AI)-based campaign in the implementation of general elections. **International Journal of Multidisciplinary Research** Review, 9 (2), 2024, pp. 117-127.

BALAGUER CALLEJÓN, F. **La constitución del algoritmo**. Río de Janeiro: Forense, 2023.

BARBOSA, L. P. La nueva orden ejecutiva de EE. UU. sobre Inteligencia Artificial segura y fiable. **Jota.** Disponible en: [https://www.jota.info/opiniao-e-analise/colunas/regulando-a-inovacao/a-nova-ordem-executiva-dos-eua-sobre-inteligencia-artificial-segura-e-confiavel]. Consultado: 13.9.2024.

BARCELLOS, A. P. de; TERRA, F. M. La libertad de expresión y los retos de la democracia digital. En: BRANCO, P. G. G.; FONSECA, R. S.; BRANCO, P. H. de M. G.; VELLOSO, J. C. B.; FONSECA, G. C S. **Eleições e democracia na era digital**. São Paulo: Almedina, 2022, p. 263-286.

BARLK, S. La ley de IA no puede prescribir consecuencias penales para las infracciones. **Indian Express.** Disponible en: [https://indianexpress.com/article/business/ai-law-

may-not-prescribe-penal-consequences-for-violations-9457780]. Consultado: 17.10.2024.
BARROSO, L.V. B. **Libertad de expresión y democracia en la era digital**. El impacto de las redes sociales en el mundo contemporáneo. Belo Horizonte: Fórum, 2023.
BENDER, S. M. L. Elecciones algorítmicas. **Michigan Law Review**, v. 121, Issue 3, p. 489-522 (2022).
BIONI, B.; GARROTE, M.; GUEDES, P. **Temas centrales en la regulación de la IA**: lo local, lo regional y lo global en la búsqueda de la interoperabilidad regulatoria. São Paulo: Asociación Brasileña de Investigación sobre Privacidad de Datos, 2023.
BOZKURT, B. Policy reccomendations for Electoral Management Bodies. **Election Monitor AI**, 1º de março de 2024. Disponível em: [https://electionmonitorai.com/2024/03/01/policy-recommendations-for-electoral-management-bodies/]. Acesso: 23.10.2024.
CARETTI, P; DE SIERVO, U. **Diritto Costituzionale e Publico.** 3 ed. Turín: G. Giappichelli, 2017.
Carter Center. **Carter Center Election Expert Mission to Kenya 2022.** Final Report. Disponible en: [https://www.cartercenter.org/resources/pdfs/news/peace_publications/election_reports/kenya-2022-elections-final-report.pdf]. Consultado: 29.10.2024.
CARRASCÓN, I. Operaciones encubiertas y usos malintencionados de la IA para influir en las elecciones. **Newtral**, 7 de octubre de 2024. Disponible en: [https://www.newtral.es/ia-influencia-elecciones/20241007/]. Consultado: 08.10.2024.
CHAKRAVARTI, J. AI-Generated Deepfakes Flood South Korean Election Campaigns. **Bank Info Security**, 20 de febrero de 2024. Disponible en: [https://www.bankinfosecurity.asia/aigenerated-deepfakes-flood-south-korean-election-campaigns-a-24399]. Consultado: 17.10.2024.
CHARAUDEAU, P. **La conquista de la opinión pública**. São Paulo: Contexto, 2016.
CHENNUPATI, A. K. The threat of artificial intelligence to elections worldwide: a review of the 2024 landscape. **World Journal of Advanced Engineering Technology and Sciences**, 2024, 12(01), pp. 29-34.
COIMISIÚN TOGHCHÁIN. **Framework on Online Process Information, Political Advertising and Deceptive AI Content**. Disponible en: [https://cdn.electoralcommission.ie/app/uploads/2024/04/23163750/Framework-on-Online-Electoral-Process-Information-Political-Advertising-and-Deceptive-AI-content.pdf]. Consultado: 23.10.2024.
CUPAĆ, J.; SCHOPMANS, H.; TUNCER-EBERTÜRK, I. Democratisation in the age of artificial intelligence: introduction to the special issue. **Democratisation**, v. 31, n. 5, 2024, pp. 899-921.
DEEPAK, P.; SIMOES, S.; MACCARTHAIGH, M. AI and core Electoral processes: mapping the horizons. **AI Magazine**, v. 44, Issue 3, September 2023, pp. 218-239.
DEGLI-ESPOSTI, S. **La ética de la inteligencia artificial**. Madrid: CSIC, 2023.
DINAMARCA, J. El riesgo de la inteligencia artificial para la democracia y los primeros esfuerzos de la UE para regularla. **The Lawyer Quarterly**, vol. 14, n. 1, 2024. Disponible en: [The Lawyer Quarterly (cas.cz)]. Consultado: 22.03.2024.
DHILLON, A. India confronts Google over Gemini AI tool's 'fascist Modi' responses. **The Guardian**, 26 de febrero de 2024. Disponible en: [https://www.theguardian.com/world/2024/feb/26/india-confronts-google-over-gemini-ai-tools-fascist-modi-responses]. Consultado: 21.10.2024.
DURAND, T. C. **Bulos, choradas e ideas perniciosas**. La ciencia detrás de las mentiras que nos cuentan. Barcelona: Plataforma Actual, 2023.

DUTT, B. Los políticos indios llevan a los muertos a la campaña electoral, con ayuda de la IA. Resto del mundo. Disponible en: [https://restofworld.org/2024/dead-relatives-ai-deepfake-india/]. Consultado el 17.10.2024.

EIFERT, M. The German Social Media Enforcement Improvement Act [NetzDG] and platform regulation. En: ABBOUD, G.; NEY JR., N.; CAMPOS, R. (eds.). **Fake News and regulation**. 2. ed. São Paulo: RT, 2020, pp. 161-191.

ESTARQUE, M.; ARCHEGAS, J. V. **Redes sociales y moderación de contenidos**: creando reglas para el debate público desde la esfera privada. Río de Janeiro: ITS-Rio, 2022.

FACHIN, J.; VERONESE, A. Ampliando el debate sobre el Artículo 19 de la Carta de Derechos de Internet de Brasil a partir de una revisión bibliográfica de la Sección 230 del Título 47 del Código de los Estados Unidos. En: FRAZÃO, A; MULHOLLAND, C; POLIDO, F. Bertini P. **Marco Civil da Internet**. Impactos, evoluciones y perspectivas. 10 anos. São Paulo: Revista dos Tribunais, 2024, pp. 43-63.

FARINHO, D. S. Delimitación del espectro normativo de las redes sociales. En: ABBOUD, G.; NEY JR., N.; CAMPOS, R. (eds.). **Fake News y regulación**. 2. ed. São Paulo: RT, 2020, pp. 29-90.

FILIMOWICZ, M. Introducción. En: FILIMOWICZ, M. **Deep Fakes**. Algorithms and Society. Nueva York: Routledge, 2022, p. X-XI.

FISHER, M. **La máquina del caos**. Cómo las redes sociales han reprogramado nuestras mentes y nuestro mundo. São Paulo: Todavia, 2023.

FREITAS FILHO, R; LIMA, T. M. Metodologia de análise de decisões. **Univ. Jus**, Brasília, n. 21, jul./dic. 2010, pp. 1-17.

FUX, L.; FONSECA, G. C. S. Moderación de contenidos y redes sociales: un ensayo sobre la libertad de expresión en la era digital. En: BRANCO, P. G. G.; FONSECA, R. S. da; BRANCO, P. H. de M. G.; VELLOSO, J. C. B.; FONSECA, G. C. S. **Eleições e democracia na era digital**. São Paulo: Almedina, 2022, p. 229-250.

GABRIEL, M. **Inteligência artificial**: do zero ao metaverso. São Paulo: Atlas, 2022.

GILLESPIE, T. **Custodios de Internet**. Plataformas, moderación de contenidos y las decisiones ocultas que dan forma a los medios sociales. New Haven y Londres: Yale University Press, 2018.

GOLTZMAN, E. M; LOPES, L. V. de S. Inteligencia artificial, discurso de odio y los límites de la justicia electoral: un estudio sobre la protección de la democracia. **Justiça Eleitoral em Debate**, v. 14, n. 1, 2024, pp. 65-73.

GOBIERNO DE CANADÁ. El Ministro LeBlanc presenta legislación para reforzar aún más el proceso electoral de Canadá, 20 de marzo de 2024. Disponible en: [https://www.canada.ca/en/democratic-institutions/news/2024/03/minister-leblanc-introduces-legislation-to-further-strengthen-canadas-electoral-process.html]. Consultado: 21.10.2024.

GRIJELMO, A. El arte de manipular a las multitudes. Las técnicas para mentir y controlar las opiniones se han perfeccionado en la era de la posverdad. **El País**, 28.08.2017. Disponível em: [https://brasil.elpais.com/brasil/2017/08/22/opinion/1503395946_889112.html]. Consultado: 02.09.24.

GUPTA, N.; MATHEWS, N. India's Experiments With AI in the 2024 Elections: The Good, The Bad & The In-between. Tech Policy Pres. Disponible en: [https://www.techpolicy.press/indias-experiments-with-ai-in-the-2024-elections-the-good-the-bad-the-inbetween/]. Consultado el 17.10.2024.

HAMMAR, Cecilia. Smart Elections: is AI the Next Wave in Electoral Management? **IDEA**, 20 de mayo de 2024. Disponible en: [https://www.idea.int/news/smart-elections-ai-next-wave-electoral-management]. Consultado: 23.10.2024.

HAN, B. C. **Infocracia**. Petrópolis: Vozes, 2022.

HARARI, Y. N. **Nexus**. Breve historia de las redes de información, de la Edad de Piedra a la inteligencia artificial. São Paulo: CIA, 2024.
HAWES, B.; HALL, W.; RYAN, M. ¿Puede utilizarse la inteligencia artificial para socavar las elecciones? **Web Science Trust**, septiembre de 2023. Disponible en: [https://eprints.soton.ac.uk/484562/]. Consultado: 30.09.2024.
HEALEY, J. El juez bloquea la ley de California que apuntaba a los anuncios falsos de campaña. **Los Angeles Times**, 3 de octubre de 2024. Disponible en: [https://www.latimes.com/california/story/2024-10-03/judge-blocks-california-law-that-targeted-deepfake-campaign-ads]. Consultado: 21 de octubre de 2024.
HERRERÍAS CASTRO, L. El conocimiento efectivo en la jurisprudencia del Tribunal Supremo: ¿hacia una obligación general de supervisión? En: HERNÁNDEZ SAINZ, E.; MATE SATUÉ, L. C.; ALONSO PÉREZ, M. T. **La responsabilidad civil por servicios de intermediación prestados por plataformas digitales**. A Coruña: Colex, 2023, p. 235-261.
IAU, J. Singapore seeks to fight deepfakes in elections with new laws ahead of 2025 polls. **MyNews,** 20 de septiembre de 2024. Disponible en: [https://www.scmp.com/week-asia/politics/article/3279357/singapore-seeks-fight-deepfakes-elections-new-laws-ahead-2025-polls]. Consultado: 18.10.2024.
INDIAN EXPRESS. Election Commission to parties: don't post deepfakes, misleading info on social media. **Indian** Express, 7 de mayo de 2024. Disponible en: [https://indianexpress.com/elections/election-commission-deepfakes-social-media-misinformation-mcc-9312006/]. Consultado: 21.10.2024.
INNERARITY, D. **Inteligencia artificial y democracia**. París: UNESCO, 2024.
JUNEJA, P. **Inteligencia Artificial para la Gestión Electoral**. Estocolmo: IDEA Internacional, 2024.
JUNGHERR, A.; RAUCHFLEISCH, A.; WUTTKE, A. Los usos engañosos de la Inteligencia Artificial en las elecciones refuerzan la prohibición de la IA. **Documento de trabajo**, 2024. Disponible en: [https://paperswithcode.com/paper/deceptive-uses-of-artificial-intelligence-in#:~:text=We%20propose%20a%20framework%20for%20assessing%20AI's%20impact%20on%20elections]. Consultado: 30.09.2024.
KAVANAGH, J.; RICH, M. D. **La decadencia de la verdad**. Una exploración inicial del papel decreciente de los hechos y el análisis en la vida pública estadounidense. Sacramento: Rand Corporation, 2018.
KERTYSOVA, K. Inteligencia artificial y desinformación: cómo la IA cambia la forma en que se produce, se difunde y se puede contrarrestar la desinformación. **Seguridad y Derechos Humanos**, vol. 29, 2018, pp. 55-81.
FUNDACIÓN KOFFI ANNAN. **Proteger la integridad electoral en la era digital.** Informe de la Comisión Kofi Annan sobre las Elecciones en la Era Digital. Ginebra: KAF, 2020.
KOLB, Andrew. **Elections in Kenya**. IFES Annual Report 2022. Disponible en: [https://www.ifes.org/ifes-annual-report-2022/elections-kenya]. Consultado: 29.10.2024.
KREPS, S.; KRINER, D. Cómo amenaza la IA a la democracia. **Journal of Democracy**, v. 34, Issue 4, October 2023, pp. 122-131.
LESSIG, L. The law of the horse: what cyberlaw might teach. **Harvard Law Review**, v. 113, 1999, pp. 501-546.
LEVITIN, D. **La mentira como arma política**. Madrid: Alianza Editorial, 2019.
LIMA-STRONG, C. Todos los principales proyectos de ley tecnológicos firmados y vetados por el gobernador de California. **The Washington Post**, 1 de octubre de 2004. Disponible en: [https://www.washingtonpost.com/politics/2024/10/01/all-major-tech-bills-californias-governor-signed-vetoed/]. Consultado el 21.10.2024.

LISSANU, A.; MORAGA, P.; SOBOL, I. Plataformas mediáticas, expresión y derechos humanos. **Global Constitutionalism Seminar 2024**, Yale Law School, septiembre de 2024, pp. 37-52.

LÓPEZ PONCE, J. TEPJF ofrecerá inteligencia artificial para asesorar dictámenes electorales. **Milenio**, 18 de junio de 2024. Disponible en: [https://www.milenio.com/politica/tribunal-electoral-ofrecera-ia-juicios-electorales]. Consultado: 08.10.2024.

LOZANO, I**. Son molinos, no gigantes.** Cómo las redes sociales y la desinformación amenazan nuestra democracia. Barcelona: Península, 2020.

MACHADO, R. C. R.; PORTELLA, L. C. Inteligencia artificial, elecciones y autenticidad electoral. En: SILVEIRA, M. de P. **Elecciones y nuevas tecnologías**. Datos, inteligencia artificial y (des)información. Brasília: Ethics 4AI; Instituto Brasiliense de Direito Público, 2024, pp. 573-588.

MAINZ, J. T; SØNDERHOLM, J.; UHRENFELDT, R. Artificial intelligence and the secret ballot. **AI and Society**, v. 39, 2022, pp. 515-522.

MARTINEZ-BRAWLEY, E. E. Hatespeech. A bird's eye view of a conundrum of international epidemic proportions. En: GUALDA, E. **Teorías de la conspiración y discurso del odio online en la sociedad de plataformas**. Comparación de agendas en narrativas y redes sociales sobre Covid-19, inmigrantes, refugiados, estudios de género y personas LGBTQ+. Madrid: Dykinson, 2024, pp. 43-59.

MATORUGA, E. El papel de la AI en la lucha contra las operaciones de influencia encubierta. Disponible en: [https://www.hulkapps.com/es/blogs/ecommerce-hub/el-papel-de-la-ia-en-la-lucha-contra-las-operaciones-de-influencia-encubierta]. Consultado: 08.10.2024.

MEIRINHO MARTINS, M. **Representação política. Elecciones y sistemas electorales**: una introducción. 2. ed. Lisboa: Instituto Superior de Ciências Sociais e Políticas, 2015.

MOSERO, Rose. In Kenya’s 2022 Elections, Technology and Data Protection Must Go Hand-in-Hand. Disponible en: [https://carnegieendowment.org/research/2022/08/in-kenyas-2022-elections-technology-and-data-protection-must-go-hand-in-hand?lang=en]. Consultado: 29.10.2024.

MUÑOZ, K. El año electoral de la IA: cómo contener el impacto de la inteligencia artificial. **DGAP Memo**, n.1, 2024, pp. 1-5.

NORDEN, L.; NARANG, N; PROTZMANN, L. J. States Take the Lead in Regulation AI in Elections - Within Limits. **Centro Brennan para la Justicia**, 7 de agosto de 2024. Disponible en: [https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-ai-elections-within-limits]. Consultado: 20.10.2024.

NUNES, F.; TRAUMANN, T. **Biografía del abismo**. Cómo la polarización divide a las familias, desafía a las empresas y pone en peligro el futuro de Brasil. Río de Janeiro: Harper Collins, 2023.

OGWUCHE, C.; ONAH, C. Behavioural Manipulation, Regulations and Oversight of Artificial Intelligence (AI) in Political Campaigns and Elections in Nigeria. **Nigerian Psychological Association**, Congreso Nacional, agosto de 2023. Disponible en: [https://www.researchgate.net/publication/380403967_Behavioural_Manipulation_Regulations_and_Oversight_of_Artificial_Intelligence_AI_in_Political_Campaigns_and_Elections_in_Nigeria]. Consultado: 18.10.2024.

OKOYE, F. Tackling Nigeria’s Electoral Challenges Utilising AI. **This Day**, 22 de outubro de 2024. Disponible en: [https://www.thisdaylive.com/index.php/2024/10/22/tackling-nigerias-electoral-challenges-utilising-ai/]. Consultado: 23.10.2024.

OLIVA, T. D.; TAVARES, V. P; VALENTE, M. ¿Una solución única para toda Internet? **Diagnósticos y Recomendaciones**, n. 4, septiembre de 2020. Disponible en:

[https://www.internetlab.org.br/wp-content/uploads/2020/09/policy_plataformas-conhecimento_20200910.pdf]. Consultado: 26.09.2024.
OSCE (Organization for Security and Co-operation in Europe). OSCE and Ukraine-s Central Election Comission launch chatbot to ease access to information in advance of 25 October local elections. Disponible en: [https://www.osce.org/project-coordinator-in-ukraine/466011]. Consultado: 23.10.2024.
PANDITHARATNE, M.; GIANSIRACUSA, N. Cómo la inteligencia artificial pone en riesgo las elecciones y las medidas que se requieren para protegernos. **Brennan Center**, 13 de julio de 2023. Disponible en: [https://www.brennancenter.org/es/our-work/analysis-opinion/inteligencia-artificial-pone-en-riesgo-elecciones-medidas-proteger-democracia]. Consultado: 03.10.2024.
PENAGOS RAMÍREZ, Juan Pablo. Registraduría revela cómo usará la inteligencia artificial para sistema de identificación y electoral de los colombianos. **El Tiempo**, 26 de agosto de 2024. Disponible en: [https://www.eltiempo.com/politica/partidos-politicos/registraduria-revela-como-usara-la-inteligencia-artificial-para-sistema-de-identificacion-y-electoral-de-los-colombianos-3375089]. Consultado: 23.10.2024.
PÉREZ DE LAMA, J.; SÁNCHEZ-LAULHÉ, J. Consideraciones a favor de un uso más amplio del término tecnopolítica. Sobre la necesidad de la crítica y la política del conocimiento tecnológico. En: SABARIEGO, J.; AMARAL, A. J.; SALLES, E. B. C. (Coords.). **Algoritmos**. Valencia: Tirant lo Blanch, 2020, pp.19-43.
RAMONET, I. **La era del conspiracionismo.** Trump, el culto a la mentira y el asalto al Capitolio. Buenos Aires: Siglo XXI, 2022.
ROTARU, G.; ANAGNOSTE, S; OANCEA, V. How Artificial Intelligence can influence elections: analysing the large language models (LLMs) political bias. **Actas de la 18ª Conferencia Internacional sobre Excelencia Empresarial 2024**, pp. 1-10.
RUBIO NÚÑEZ, Rafael; ALVIM, Frederico Franco; MONTEIRO, Vitor de Andrade. **Inteligencia artificial y campañas electorales algorítmicas:** Disfunciones informativas y amenazas sistémicas de la nueva comunicación política. Madrid: CEPC, 2024.
RUBIO NÚÑEZ, Rafael; MONTEIRO, Vitor de Andrade. Preserving trust in democracy: The Brazilian Superior Electoral Court's quest to tackle disinformation in elections. **South African Journal of International Affairs**. 30. 1-24. 2024. DOI 10.1080/10220461.2023.2274860.
SAFIULLAH, M.; PARVEEN, N. Big Data, Artificial Intelligence and Machine Learning: a paradigm shift in election campaigning. **The New Advanced Society**, 2021, pp. 247-261.
SÁNCHEZ MUÑOZ, O. **La regulación de las campañas electorales en la era digital.** Desinformación y microsegmentación en redes sociales con fines electorales. Madrid: Centro de Estudios Políticos y Constitucionales, 2020.
SANDEL, M J. **El descontento de la democracia.** Un nuevo enfoque para tiempos peligrosos. Río de Janeiro: Civilización Brasileña, 2023.
SAPADA, A. T.; ARIF, M. Use of Artificial Intelligence in General Elections: Comparison of Indonesian and German Regulations. **Law and Social Journal**, vol. 1, n. 1, 2024, pp. 21-40.
GOBIERNO DE SINGAPUR. Nuevas medidas legales para mantener la integridad de la publicidad en línea durante las elecciones. **Ministerio de Desarrollo Digital e Información**, 9 de septiembre de 2024. Disponible en: [https://www.mddi.gov.sg/new-legal-measures-to-uphold-integrity-of-online-advertising-during-elections/]. Consultado: 21.10.2024.
SOON, C.; QUEK, S. Salvaguardar las elecciones de las amenazas de la inteligencia artificial. **IPS Working Papers**, n. 56, agosto de 2024.

SUÁREZ, P. S. La inteligencia artificial (AI) y las elecciones: breves y primeras reflexiones sobre el uso, el impacto y la influencia de la AI en los procesos electorales. **Pensar en Derecho**, n. 22, 2023, pp. 33-51.

TAVARES, A. R. El riesgo democrático en la era digital. En: BRANCO, P. G. G; FONSECA, R. S. da; BRANCO, P. H. de M. G; VELLOSO, J. C. B.; FONSECA, G. C. S. **Eleições e democracia na era digital**. São Paulo: Almedina, 2022, p. 427-438.

TAVARES, C. de M. Inteligência artificial e deepfakes: desafios jurídicos e tecnológicos para a integridade do processo democrático e implicações para as eleições municipais de 2024. **Justiça Eleitoral em Debate**, v. 14, n. 1, 2024, pp. 49-58.TOMIĆ, Z.; DAMNJANOVIĆ, T.; TOMIĆ, I. Artificial Intelligence in Political Campaigns. **South Eastern European Journal of Communication**, vol. 5, n. 2, Winter 2023, pp. 17-28.

TUSET VARELA, Damián. Cuando la IA decide: fronteras legales y éticas de la IA em el sistema electoral. **Diario La Ley**, 2 de fevereiro de 2024. Disponible en: [https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAC2NwWrDQAxEv6Z7MRQ3PqQ97MX1MZTSmt5lWdgLm1Uqad347yuSCAaN0Ejvt5LsI10tIhcTzo0yJshNTpNQg0mwZsDEpbmQKBfQoHvhsp_jKJWCwaSxfTrii-sQAK1CHhjjzaeNRphiG1hmkn53Z2yQv0hj1x6Drvz3AVtawBzRg9yfpnmOw9h6dW_d4bULm7M9EH_SQsUorGlZTy6755VAcP2EhaKj69kz_Ax6uT42fTXz68nK920OmL0PYPQOmcr84P4DslXoVw0BAAA=WKE]. Consultado: 23.10.2024.

SLOWING-ROMERO, S.; SCRIVEN, J. Democracia, retroceso y tribunales. **Global Constitutionalism Seminar 2024**, Yale Law School, septiembre de 2024, pp. 3-18.

SOUZA NETO, C. P. de. **Democracia en crisis en Brasil.** São Paulo: Contracorrente, 2020.

STEVENSON, K. Inteligencia Artificial: un arma de doble filo en las elecciones. **Educational Administration: Theory and Practice**, 30(4), 2024, pp. 1.660-1.667.

SULEYMAN, M.; BHASKAR, M. **The next wave**: artificial intelligence, power and the greatest dilemma of the 21st century. Río de Janeiro: Record, 2024.

Gobierno británico. **A pro-innovation approach to AI regulation.** Policy Paper, 3 de agosto de 2023. Disponible en: [https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper]. Consultado el 21 de octubre de 2024.

UNDP (United Nations Development Programmes). Election Comission uses artificial intelligence to enhance women's participation in electoral processes, 9 de agosto de 2022. Disponible en: [https://www.undp.org/libya/press-releases/election-commission-uses-artificial-intelligence-enhance-womens-participation-electoral-processes]. Consultado: 23.10.2024.

UNESCO (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura). **Elecciones en la era digital.** Guía para profesionales electorales. Disponible en: [https://unesdoc.unesco.org/ark:/48223/pf0000382102]. Consultado: 21.08.2024.

VALDES ZEPEDA, A.; ARÉCHIGA, D.; DAZA MARCO, T. Inteligencia artificial y su uso en las campañas electorales en sistemas democráticos. **Revista Venezolana de Gerencia**, Año 29, n. 105, 2024, pp. 63-76.

VESTING, T. El cambio de la esfera pública por la inteligencia artificial. En: ABBOUD, G.; NEY JR., N.; CAMPOS, R. (eds.). **Fake News y regulación**. 2. ed. São Paulo: RT, 2020, pp. 193-210.

VIVAS ESCRIBANO, G. Desinformación y polarización en relación con las redes sociales. En: CARRATALÁ, A.; IRANZO CABRERA, M.; LÓPEZ GARCÍA, G. (eds.). **De la desinformación a la conspiración**. Política y comunicación en un paisaje mediático híbrido. Valencia: Tirant lo Blanch, 2023, p. 351-359.

VLACHOS, S. The link between mis-, dis-, and malinformation and domestic extremism. **Consejo de Asuntos Emergentes de Seguridad Nacional**, junio de 2022. Disponible en: [MDM_22.6.17b.pdf (censa.net)]. Consultado: 30.08.2024.

CASA BLANCA. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Disponible en: [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/]. Consultado: 21.10.2024.

FORO ECONÓMICO MUNDIAL. Informe sobre Riesgos Mundiales 2024: Insight Report, 19ª edición. Enero de 2024.

YAZBEK, S. Inteligencia artificial aplicada a los procesos electorales. **Instituto Democracia y Elecciones**, 27 de abril de 2024. Disponible en: [https://idemoe.org/la-inteligencia-artificial-aplicada-a-procesos-electorales-desafios-de-la-observacion-electoral/]. Consultado: 03.10.2024.

YU, C. ¿Cómo nos robará la IA las elecciones? **Centro para la Ciencia Abierta**, OSF Preprints, 2024, pp. 01-24.

ZACHARY, G. P. Digital manipulation and the future of Electoral democracy in U.S. **IEEE Transactions on Technology and Society**, v. 1, n. 2, June 2020, pp. 104-112.