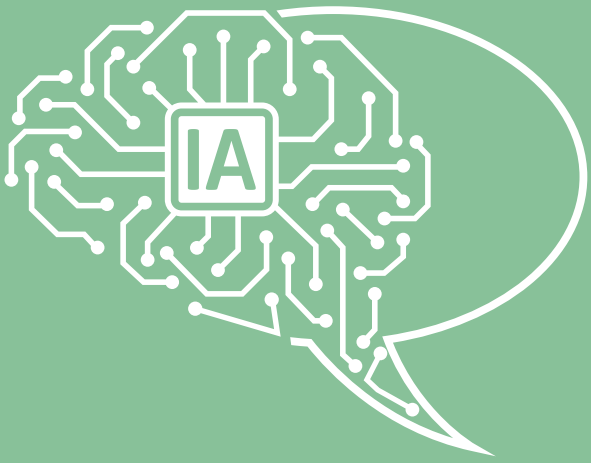
Justicia electoral cercana:
diálogos sobre nuestra democracia

TRIBUNAL ELECTORAL
del Poder Judicial de la Federación

ANUIES
Asociación Nacional de Universidades e Instituciones de Educación Superior



Democracia entre algoritmos

Inteligencia artificial, plataformas digitales y justicia electoral

Volumen IV



Democracia entre algoritmos

Inteligencia artificial, plataformas digitales y justicia electoral

Volumen IV

Editorial
TEPJF

Justicia electoral cercana:
diálogos sobre nuestra democracia

Democracia entre algoritmos

Inteligencia artificial, plataformas digitales y justicia electoral

Volumen IV

TRIBUNAL ELECTORAL
del Poder Judicial de la Federación

ANUIES
Asociación Nacional de Universidades e Instituciones de Educación Superior

México, 2026

342.07
B333j Bátiz García, Gilberto de Guzmán; González Placencia, Luis Armando.
Justicia electoral cercana : diálogos sobre nuestra democracia / Gilberto de Guzmán Bátiz García. -- 1.ª edición. -- Ciudad de México, México : Tribunal Electoral del Poder Judicial de la Federación ; Asociación Nacional de Universidades e Instituciones de Educación Superior de la República Mexicana, 2026.
4 volúmenes ; 21 cm

Contenido: Volumen I. Del litigio al diálogo en la justicia electoral : mecanismos alternativos, mediación y paz democrática -- Volumen II. Elecciones judiciales en México : el nuevo paradigma democrático -- Volumen III. Representación, inclusión y pluralismo : pueblos indígenas, grupos de atención prioritaria y justicia electoral -- Volumen IV. Democracia entre algoritmos : inteligencia artificial, plataformas digitales y justicia electoral.

ISBN TEPJF obra completa: en trámite.
ISBN TEPJF del volumen IV: en trámite.
ISBN ANUIES obra completa: en trámite.
ISBN ANUIES del volumen IV: en trámite.

1. Derecho electoral - México. 2. Justicia electoral - México. 3. Democracia - México. 4. Derechos político-electorales - México. I. Bátiz García, Gilberto de Guzmán. II. Tribunal Electoral del Poder Judicial de la Federación. III. Asociación Nacional de Universidades e Instituciones de Educación Superior de la República Mexicana. IV. Título.

Justicia electoral cercana: diálogos sobre nuestra democracia
Volumen IV. *Democracia entre algoritmos. Inteligencia artificial, plataformas digitales y justicia electoral*

1.ª edición, 2026.

D. R. © Tribunal Electoral del Poder Judicial de la Federación.
Carlota Armero 5000, CTM Culhuacán,
04480, Coyoacán, Ciudad de México.
Teléfono: 55-5728-2300.
www.te.gob.mx
editorial@te.gob.mx

© 2026, ANUIES.
Tenayuca 200, Col. Santa Cruz Atoyac,
Alcaldía Benito Juárez, C.P. 03310, Ciudad de México.

ISBN obra completa: en trámite.
ISBN volumen IV: en trámite.

ISBN obra completa: en trámite.
ISBN volumen IV: en trámite.

Edición: Dirección General de Documentación.

Las opiniones expresadas en la presente obra son responsabilidad exclusiva de quienes las emiten.

Esta publicación es de distribución gratuita. Prohibida su venta.
Consulta y descarga libre en www.te.gob.mx/editorial

Editorial TEPJF

DESCARGA GRATUITA

Directorio

Sala Superior

Magistrado Gilberto de G. Bátiz García
Presidente

Magistrado Felipe Alfredo Fuentes Barrera
Magistrado Felipe de la Mata Pizaña
Magistrado Reyes Rodríguez Mondragón
Magistrada Claudia Valle Aguilasocho

Comité Académico

Magistrado Gilberto de G. Bátiz García
Presidente

Magistrado Felipe Alfredo Fuentes Barrera
Magistrado Felipe de la Mata Pizaña

Dra. Fabiola Martínez Ramírez
Dr. Hugo Saúl Ramírez García
Dra. Gloria Ramírez Hernández
Dra. Laura Guadalupe Zaragoza Contreras

Dr. Luis Octavio Vado Grajales
Secretario Técnico Académico

Lic. Agustín Millán Gómez
Secretario Técnico Editorial

Directorio

Asociación Nacional de Universidades e Instituciones de Educación Superior

Luis Armando González Placencia
Secretario General Ejecutivo

Gustavo Rodolfo Cruz Chávez
Coordinador General de Vinculación Estratégica

Luis Alberto Fierro Ramírez
Coordinador General de Fortalecimiento Académico e Institucional

Irma Andrade Herrera
Coordinadora General de Planeación y Buena Gestión

José Luis Cuevas Nava
Director Ejecutivo de Publicaciones y Fomento Editorial

Índice

11 Presentación

15 Prólogo

21 Introducción

33 Coordenadas jurídicas

55 Diálogos regionales

101 Análisis transversal

115 Agenda para la justicia electoral

129 Conclusiones

137 Referencias

147 Anexo metodológico



Presentación



La colección *Justicia electoral cercana: diálogos sobre nuestra democracia* nace de una convicción institucional compartida por el Tribunal Electoral del Poder Judicial de la Federación y la Asociación Nacional de Universidades e Instituciones de Educación Superior. La justicia electoral no puede limitarse a resolver expedientes desde la distancia; debe escuchar, comprender, dialogar y explicar los problemas reales de la democracia mexicana.

La idea de justicia electoral cercana no debe entenderse solo como presencia territorial. Es, ante todo, un método de trabajo del servicio público. Significa mirar los conflictos electorales desde su contexto, reconocer las realidades locales, construir puentes con la academia, conversar con tribunales, autoridades y ciudadanía, así como traducir las decisiones jurisdiccionales a un lenguaje que permita comprender por qué importan para la vida democrática.

La primera etapa de este proyecto fue la celebración de seis seminarios regionales, cuyo valor metodológico es central. No se trató de foros unidireccionales ni de actos protocolarios. Fueron espacios horizontales de diálogo en los que participaron autoridades administrativas y jurisdiccionales, integrantes de las universidades, especialistas y organizaciones sociales. Esa metodología permitió que la colección no surgiera solo desde el centro, sino desde una conversación nacional, plural y contextual.

En ese sentido, los seminarios cumplieron una función doble: por un lado, permitieron identificar preocupaciones comunes en distintas regiones del país; por otro, hicieron visible que la justicia electoral enfrenta dilemas que no pueden resolverse solo con categorías abstractas. Cada territorio aporta preguntas, experiencias, tensiones y aprendizajes propios. La colección busca preservar ese diálogo y convertirlo en una herramienta de reflexión pública.

Este volumen aborda la relación entre inteligencia artificial, plataformas digitales y justicia electoral. Su contenido analiza cómo la democracia se desenvuelve hoy en entornos digitales que inciden en la propaganda, la deliberación pública, la libertad

de expresión, la violencia política en línea, la prueba electoral, la microsegmentación, la responsabilidad de las plataformas, la autenticidad de contenidos y el uso institucional de herramientas tecnológicas.

El tema importa porque la democracia ya no se juega solo en casillas, partidos políticos, calles, plazas y medios de comunicación tradicionales. También se desenvuelve en bases de datos, algoritmos, redes sociales, anuncios personalizados, mensajes automatizados y contenidos generados por inteligencia artificial. Ignorar ese entorno sería llegar tarde a los conflictos que marcarán los próximos procesos electorales del país.

El desafío para la justicia electoral consiste en no reaccionar con recelo ni entusiasmo irreflexivos ante toda innovación tecnológica. Es decir, debe evitar dos extremos: por un lado, el pánico tecnológico, que puede conducir a restricciones desproporcionadas al debate público digital y, por el otro, la ingenuidad regulatoria, que puede dejar sin respuesta dinámicas tecnológicas capaces de afectar los derechos, la equidad, la autenticidad informativa y la confianza ciudadana.

La justicia electoral cercana adquiere aquí una dimensión inédita. Debe ser capaz de entender cómo se informa la ciudadanía, cómo circula la propaganda, cómo se construyen percepciones, cómo se acredita una infracción en entornos digitales y cómo se protegen derechos sin inhibir la libertad de expresión.

Este volumen invita a construir una justicia electoral preparada para el futuro: una justicia que comprenda la tecnología, pero que no pierda su brújula constitucional; una justicia que gobierne los nuevos riesgos democráticos con principios, evidencia, transparencia y responsabilidad pública.

Gilberto de G. Bátiz García
Magistrado presidente
de la Sala Superior del Tribunal Electoral
del Poder Judicial de la Federación

Luis Armando González Placencia
Secretario General Ejecutivo de la Asociación Nacional
de Universidades e Instituciones de Educación Superior



Prólogo



El sistema democrático en México —al igual que en el resto del mundo— se enfrenta a una crisis de adaptabilidad que amenaza directamente su legitimidad. La proliferación de la inteligencia artificial y el auge de las plataformas digitales ya no son tecnologías del futuro, sino fuerzas disruptivas que moldean activamente la comunicación política y la percepción pública de los candidatos. Ante este escenario, la democracia mexicana está obligada a evolucionar: debe adoptar estas herramientas digitales no solo para blindar la confianza ciudadana, sino para dotar de una eficiencia inédita a la impartición de justicia.

La obra en análisis forma parte de la colección *Justicia electoral cercana: diálogos sobre nuestra democracia*, lo que constituye un esfuerzo conjunto del Tribunal Electoral del Poder Judicial de la Federación (TEPJF) y la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) para acercarse a los temas de controversia e interés más relevantes que, en materia electoral, ocupan buena parte de la labor jurisdiccional y de su visión hacia el futuro. Dicho esfuerzo nos permite focalizar la atención en los asuntos que requieren mayor atención y replantearnos nuestra posición sobre aspectos y problemáticas en constante cambio para ofrecer respuestas y soluciones novedosas a situaciones de vanguardia, especialmente a la luz de las constantes transformaciones tecnológicas que impactan en la sociedad y, por ende, redefinen la lógica de los procesos electorales.

Bajo esta premisa, la obra examina a fondo las directrices normativas que configuran el sistema de justicia electoral. El texto desentraña los criterios y estándares indispensables para trazar una doble estrategia institucional: primero, incentivar y blindar el uso de herramientas digitales para modernizar la labor judicial; segundo, contener y erradicar con firmeza aquellas conductas que distorsionan la competencia y erosionan la confianza ciudadana en la democracia.

Definir este marco normativo no es un asunto menor; de ello depende que la inteligencia artificial sirva a la democracia y no en su contra. La regulación propuesta por la obra busca resolver

problemas críticos: desde combatir la opacidad de las plataformas digitales que distorsionan la competencia, hasta frenar la desinformación que manipula el voto. Sin embargo, el texto nos recuerda con acierto que las leyes no operan en el vacío. La viabilidad de este modelo recae, en última instancia, en la corresponsabilidad entre el legislador, encargado de crear las leyes, y las autoridades administrativas, responsables de ejecutar los mandatos abstractos.

Entre los aportes más significativos del texto destaca el diagnóstico de la transición que vive la justicia electoral en México. Históricamente, las prioridades del diseño institucional estuvieron volcadas en la construcción de certeza jurídica, el control del escrutinio, la defensa de los derechos políticos y la regulación de los medios masivos tradicionales. Si bien estos pilares éticos permanecen intactos, el ecosistema digital exige una reconfiguración regulatoria. El reto contemporáneo ya no es solo procedimental, sino estructural: la justicia electoral debe blindar la equidad y el voto libre frente a los sesgos tecnológicos, impidiendo que la función pública del Estado termine subordinada a los intereses y dinámicas de los gigantes tecnológicos privados.

En este contexto, el análisis adquiere una dimensión pragmática al reconocer que, ante la ausencia de un marco normativo vigente que regule eficazmente la inteligencia artificial en los procesos electorales, el órgano jurisdiccional ha tenido que recurrir a la comparación jurídica internacional. La obra demuestra cómo las principales directrices de protección provienen de los criterios y resoluciones emanadas de decisiones judiciales y tribunales de otras latitudes. A partir de este enfoque, el texto se aboca al estudio de casos prácticos y debates regionales sobre la implementación de sistemas algorítmicos en el ámbito electoral. Entre estos, destacan tres vertientes fundamentales: la instrumentación de algoritmos para salvaguardar la equidad en la contienda, su aplicación técnica en la valoración de elementos probatorios y los imperativos éticos y pedagógicos que demandan su adopción.

En consecuencia, el libro establece que los logros más relevantes de estos ejercicios constituyen la consolidación de canales institucionales claros, plazos de respuesta, protocolos de solicitud, mecanismos de emergencia, comunicación con organismos públicos locales electorales y tribunales locales, así como criterios uniformes para atender la violencia política, la desinformación y la interferencia electoral.

Más allá del diagnóstico, la obra asume un compromiso propositivo al trazar la ruta que debe seguir la justicia electoral mexicana. Su tesis central exige un balance audaz: es imperativo defender las libertades que han dado vida a nuestra democracia —el debate vivo, la crítica abierta y la creatividad política— al mismo tiempo que se

construyen diques de contención contra el uso malicioso de la tecnología. Ignorar este dilema significaría permitir que las herramientas digitales socaven los cimientos de la confianza pública.

En este orden de ideas, del ejercicio analítico realizado en la obra se concluye que la democracia mexicana opera en un entorno fuertemente definido por los algoritmos digitales, que conducen la opinión y el posicionamiento ideológico de una parte significativa de la sociedad hacia puntos determinados; en este sentido, las redes sociales, los motores de recomendación, la publicidad digital y las plataformas privadas forman parte del ecosistema ordinario de las campañas. Sin embargo, este resultado cuenta con un importante matiz: no toda la realidad nacional opera de la misma manera, pues, dependiendo de la región, los datos fluctúan, por lo que la justicia electoral debe buscar adaptarse no solo a los nuevos retos, sino a las diferentes realidades regionales.

Hacia el final de la obra, se defiende que una de las conclusiones más importantes es que se identifica a la autenticidad como bien democrático, consistente en que la ciudadanía se debe encontrar en capacidad de verificar si la información a la que se expone de manera voluntaria e involuntaria corresponde a personas reales, hechos verificables u opiniones humanas; si se trata de una edición o de contenido fabricado.

La seguridad tecnológica de los procesos electorales, el uso de la inteligencia artificial por las autoridades y la erosión de la confianza en el sistema electoral y democrático también son cuestiones de estudio interesantes que definen el debate actual, pues todos estos elementos pueden generar factores de riesgo para la democracia en el supuesto de verse vulnerados o, en su caso, materializados. De ahí la importancia de buscar que ninguno de los supuestos se actualice a fin de mantener la estabilidad de la democracia actual.

Un razonamiento medular de la obra es que la tecnología y los ecosistemas digitales no deben conceptualizarse como cuerpos extraños al sistema democrático. En su lugar, el texto propone un modelo de coexistencia regulatoria. Esta visión exige un equilibrio preciso: instrumentalizar las herramientas digitales bajo el amparo de la libertad, explotar su eficiencia sin abdicar de la soberanía ciudadana en las decisiones públicas y blindar el proceso frente a malas prácticas sin que ello implique un retroceso en el desarrollo tecnológico.

A modo de conclusión, el trabajo ofrece cuestiones determinantes sobre el futuro de la democracia y su vinculación con la inteligencia artificial y las nuevas tecnologías. Parte del hecho de que actualmente la integridad de una elección no depende solo de la jornada, el cómputo o la fiscalización de gastos, sino también del contexto y el

entorno informativo del proceso, lo cual puede afectar decisivamente una elección sin incidir activamente durante la jornada electoral y configurar con ello una vulneración al principio de equidad en la contienda.

En este sentido, la obra esboza, de manera magistral y consciente de sus responsabilidades, que parte de los esfuerzos del TEPJF deben estar dirigidos a construir una doctrina constitucional sobre integridad informativa, autenticidad del debate público, responsabilidad digital, trazabilidad de contenidos y protección de la autonomía del voto. De igual manera, este órgano jurisdiccional debe definir los protocolos de uso de la inteligencia artificial y las plataformas digitales, auditoría, supervisión, protección de datos, verificación de resultados y límites frente a tareas sustantivas.

Este despliegue institucional no puede ser aislado: los esfuerzos del Tribunal Electoral del Poder Judicial de la Federación deben articularse con la participación de los partidos políticos y las demás autoridades electorales. Esta alianza es indispensable para un doble propósito: salvaguardar la integridad del proceso y promover un uso ético y responsable de los ecosistemas virtuales. Paralelamente, resulta imperativo diseñar un marco normativo especializado en materia de inteligencia artificial y elecciones; un modelo legislativo dotado de la flexibilidad y resiliencia necesarias para adaptarse a las vertiginosas transformaciones tecnológicas de nuestro tiempo.

Considero que la obra es un material excelente y de lectura obligada para quienes actuamos como agentes activos dentro del sistema electoral mexicano, ya que nos ayuda a dilucidar nuestro papel en un entorno electoral en constante transformación. En este sentido, debemos ampliar la perspectiva para comprender que la integridad de la jornada comicial puede verse comprometida desde etapas previas debido al uso de herramientas tecnológicas. Sin embargo, la respuesta no debe ser la obstaculización de estos recursos, sino su adecuada implementación por parte de los órganos jurisdiccionales, las instituciones electorales y los partidos políticos como usuarios responsables.



Introducción



La democracia constitucional contemporánea enfrenta una transformación profunda en las condiciones materiales de su deliberación pública. Durante buena parte del siglo XX, los procesos electorales se organizaron alrededor de partidos políticos, medios de comunicación masivos, propaganda, encuestas, jornadas electorales y mecanismos jurisdiccionales para resolver controversias. Ese mundo no ha desaparecido, sigue siendo decisivo; pero el ecosistema en el que se forma la opinión pública, circula la información política, se construyen identidades electorales y en el que se disputa la confianza ciudadana ya no es el mismo.

El cambio no puede explicarse solo como el tránsito de una comunicación analógica a otra digital. Lo que está sucediendo es más complejo: es una reorganización de la esfera pública a partir de plataformas privadas, sistemas algorítmicos, grandes bases de datos, publicidad digital, grandes modelos de lenguaje, sistemas de recomendación, redes de mensajería instantánea, moderación automatizada y producción sintética de contenidos. Es decir, la conversación democrática se desenvuelve ahora también en un espacio con cada vez más influencia, mediado por tecnologías que no solo transmiten mensajes, sino que los clasifican, priorizan, amplifican, segmentan, personalizan, monetizan y, ahora, en la mayoría de los casos, los crean.

La pregunta, en este contexto, es: ¿cómo asegurar elecciones libres, auténticas, equitativas e íntegras cuando buena parte de la información política se produce, circula y se recibe en entornos digitales gobernados por lógicas algorítmicas y comerciales que en principio no fueron diseñadas para potenciar o proteger los derechos político-electorales?

Este volumen, de la colección *Justicia electoral cercana*, descansa en esta premisa central: la inteligencia artificial (IA) y las plataformas digitales no constituyen un tema accesorio de la dinámica democrática; son ya parte del contexto en el que se ejercen derechos políticos, se desenvuelve la competencia electoral, se produce y difunde propaganda política, se despliegan campañas de desprestigio, se amplifican discursos discriminatorios y de

violencia política, se construyen narrativas de fraude y se definen las condiciones del voto informado.

La justicia electoral debe entender este nuevo mundo de la participación y la expresión política. En buena medida, de eso depende ahora proteger derechos, garantizar la legalidad, preservar la equidad, sancionar infracciones y ofrecer razones públicas capaces de sostener la confianza democrática.

Ahora bien, la discusión en torno a este cambio tecnológico y los procesos electorales es amplia y compleja; hoy, cada una de las sociedades democráticas reflexiona acerca de cómo sortear los principales retos que plantea esta transformación en la esfera pública. No obstante, y para efectos de esta introducción, se puede ordenar en tres planos clave.

El primero es tecnológico: la IA generativa y las plataformas digitales han modificado las capacidades de producción, distribución y personalización de información política. Luego, está el plano democrático-electoral: estas herramientas generan oportunidades, pero también riesgos para la integridad informativa, la equidad de la contienda, la libertad del voto, la certeza, la privacidad, la no discriminación, la confianza pública y la legitimidad electoral.

Y, por último, es indispensable sumar la perspectiva normativa. Las democracias deben construir reglas, criterios jurisdiccionales, capacidades institucionales y estándares de responsabilidad que permitan enfrentar estos riesgos sin sacrificar la libertad de expresión, el pluralismo ni la crítica política.



La discusión sobre IA y elecciones suele enfocarse en imágenes falsas, audios clonados, videos manipulados o propaganda generada por sistemas automatizados. Los *deepfakes* (imágenes, videos o audios hiperrealistas generados con IA que imitan la apariencia y la voz de una persona para hacerla decir o hacer algo que no sucedió) y otros contenidos sintéticos producen alarma porque alteran la relación ordinaria entre prueba, percepción y realidad. Una imagen o un audio de apariencia verosímil puede atribuir a una persona candidata palabras, gestos, acciones y contextos que nunca ocurrieron. Esto, en procesos electorales, en los que el tiempo de reacción es breve ante lo sumario de sus procedimientos y el daño reputacional puede ser inmediato, es una capacidad técnica con riesgos no menores que son evidentes.

Sin embargo, centrar o reducir el problema a los *deepfakes,* a la microsegmentación política, al *astroturfing* (contenido sintético que puede incluir *bots* o granjas de *trolls* para generar campañas organizadas y financiadas con la finalidad de alterar la percepción de la opinión pública) y a la desinformación intencional no es atinado. La IA no incide en la política solo cuando produce una pieza falsa de propaganda; está presente en capas más profundas del ecosistema informativo, las cuales le dan estructura y lógica. Las plataformas digitales utilizan sistemas algorítmicos para ordenar contenidos, recomendar publicaciones, decidir qué aparece en la pantalla de cada persona usuaria, moderar discursos, distribuir publicidad, segmentar audiencias y maximizar la interacción. No obstante, aun antes de la popularización de la IA generativa, la vida pública ya estaba mediada por sistemas automatizados.

La novedad de los últimos años consiste en la convergencia de, por lo menos, dos cambios clave: la irrupción, en primer lugar, de las plataformas digitales como máquinas de distribución y amplificación del contenido de sus usuarios mediante herramientas inteligentes automatizadas, y la posterior llegada de los modelos de IA generativa accesibles a millones de personas y organizaciones, lo que permite a su vez producir texto, imagen, audio y video sintéticos a muy bajo costo, a gran velocidad y que se pueden escalar fácilmente. Esto ha implicado que, por un lado, las campañas políticas puedan integrar estas herramientas a sus operaciones cotidianas, al redactar mensajes, producir materiales, analizar audiencias, generar propaganda, probar narrativas o automatizar interacciones y, por el otro, que actores maliciosos puedan utilizar las mismas tecnologías para suplantar identidades, fabricar evidencia, crear redes falsas de apoyo, hostigar candidaturas o inducir a la confusión.

La literatura acerca de campañas identifica al menos tres grandes usos de la IA en procesos electorales. El primero, como ya se apuntó, corresponde a operaciones internas de campaña; esto es, redactar discursos, mensajes, notas, organizar bases de datos, comunicación con voluntarios, entrenar equipos de trabajo y eficientizar la estructura organizacional. Luego está el contacto con votantes; es decir, personalizar mensajes, segmentar audiencias, ajustar narrativas acordes con las necesidades y los intereses de cada persona o grupo, administrar *chatbots* de campaña, etcétera. El tercero comprende usos engañosos: crear o distribuir *deepfakes*, suplantar identidades, realizar *astroturfing*, crear contenidos falsos, operar redes de *bots*, manipular evidencia o mensajes diseñados para ocultar información (Foos, 2024; Jungherr *et al*., 2026).

Esta distinción es útil porque evita una discusión simplista sobre la IA. No todos sus usos tienen un impacto negativo y, en su caso, la gravedad de estos no es igual en todos los casos. Un partido político que utiliza IA para resumir documentos internos o traducir materiales de campaña enfrenta un riesgo muy distinto al de una candidatura que crea y difunde un audio sintético atribuido falsamente a su adversario. Un *chatbot* que ofrece información pública sobre propuestas electorales no plantea la misma responsabilidad que una red automatizada que simula apoyo ciudadano inexistente.

El uso de la IA no es, por sí mismo, una infracción electoral. Sí puede ser un medio para cometer infracciones a la legislación electoral, pero también puede aprovecharse válidamente como instrumento de organización, herramienta de comunicación, técnica de segmentación, así como mecanismo de accesibilidad. En este sentido, el análisis jurídico debe focalizarse en aspectos como los usos, riesgos, sujetos, efectos y bienes jurídicos comprometidos. Lo relevante, desde el ámbito jurídico, reside en para qué se usó, quién la utilizó, con qué grado de transparencia, con qué efectos sobre derechos o principios electorales y en qué condiciones de responsabilidad.

El problema democrático no reside solo en que existan contenidos falsos, sino en la forma en que esos contenidos se distribuyen, amplifican y reciben. Un *deepfake* aislado puede tener poco impacto. Pero un contenido falso amplificado por redes coordinadas, insertado en comunidades polarizadas, distribuido en momentos críticos de campaña y reforzado por microsegmentación puede producir efectos más graves: confusión, descrédito institucional, intimidación, desaliento del voto o consolidación de narrativas de fraude. El uso de *bots,* cuentas automatizadas, redes coordinadas y operaciones de influencia precede a la expansión de la IA generativa. Algunos estudios sobre el caso mexicano han mostrado que, desde hace años, hay presencia de *bots* y demás estrategias de propaganda política digital en la conversación pública; propaganda vinculada con ataques a adversarios, promoción de figuras políticas, creación artificial de apoyos, distorsión de tendencias y circulación de información engañosa. La IA generativa se inserta en ese terreno preexistente. No inaugura de cero la manipulación digital; la dota de nuevas y extraordinarias capacidades (Ramírez *et al.,* 2025).

¿Cómo evaluar y determinar los riesgos democráticos de la IA y las plataformas digitales? Una buena guía normativa, acorde con las reglas electorales constitucionales, legales y administrativas, puede ser la integridad electoral. En efecto, una elección íntegra exige condiciones de competencia equitativa, información veraz, libertad de sufragio, ausencia de violencia, transparencia, rendición de cuentas, imparcialidad de las autoridades y confianza pública en el proceso. Y justo la IA y las plataformas digitales pueden afectar cualquiera de estos aspectos.

El primer riesgo, en este sentido, es la degradación informativa. Las elecciones requieren información veraz sobre candidaturas, partidos, propuestas, reglas, fechas, lugares de votación, resultados, autoridades, vías de impugnación, etcétera. Cuando circulan contenidos falsos, manipulados o engañosos sobre estos elementos, se afecta la capacidad ciudadana de participar en condiciones de autonomía. La IA generativa y los intermediarios digitales pueden producir y distribuir desinformación a escala, adaptar mensajes a grupos específicos y fabricar materiales con apariencia de autenticidad. Esto puede impactar de forma engañosa en la formación de preferencias y, a su vez, generar confusión sobre procedimientos, desincentivar la participación o alimentar narrativas de fraude.

Otro riesgo es la suplantación de identidad. La posibilidad de fabricar voces, rostros o estilos comunicativos permite atribuir falsamente declaraciones o conductas a candidaturas, autoridades, periodistas, personas juzgadoras o liderazgos sociales. En una campaña, un audio sintético difundido horas antes de la jornada puede producir un daño que una rectificación posterior no logre reparar en la dinámica político-electoral. Esta práctica puede afectar el honor y reputación de ciertas personas, pero también es capaz de alterar la percepción ciudadana sobre idoneidad, integridad, posturas políticas o conducta respecto de una candidatura.

El siguiente riesgo no es menor: la microsegmentación de la discusión pública. La publicidad política dirigida puede ser legítima cuando informa, moviliza y permite la comunicación eficiente. Pero se vuelve problemática si se basa en datos personales sensibles, si oculta mensajes contradictorios, si explota vulnerabilidades emocionales, si impide el escrutinio público y si permite que cada grupo reciba una versión distinta de la realidad respecto de la discusión pública, el proceso electoral o las candidaturas en competencia. La opacidad de la segmentación limita la fiscalización social y fragmenta

el debate democrático; las promesas dejan de ser públicas y se convierten en mensajes privados para audiencias específicas.

El cuarto riesgo es la violencia política amplificada. La IA puede utilizarse para producir contenidos misóginos, racistas, homofóbicos, clasistas o discriminatorios. En América Latina, los estudios sobre IA e integridad informativa advierten que las mujeres, las personas de la diversidad sexual y otros grupos de atención prioritaria históricamente excluidos pueden enfrentar daños específicos mediante imágenes no consentidas, sexualización, ridiculización, discursos de odio o ataques a su legitimidad pública. En contextos en los que la violencia política contra las mujeres o contra grupos de atención prioritaria ya es un problema estructural, la IA puede abaratar y multiplicar las agresiones (International Institute for Democracy and Electoral Assistance y Fundação Getulio Vargas Comunicação, 2025).

Otro escenario que no hay que descartar es la erosión de la confianza pública. La democracia requiere una confianza mínima en que los hechos básicos pueden conocerse, en que las autoridades actúan conforme a las reglas y en que los resultados electorales tienen un procedimiento verificable. La proliferación de contenidos sintéticos puede producir no solo engaño, sino incertidumbre generalizada. Cuando todo puede ser falso, también lo verdadero puede ser negado como fabricación. Este fenómeno permite que actores acusados de conductas reales aleguen manipulación, y que actores maliciosos exploten la duda para debilitar la rendición de cuentas. La afectación no recae solo en la información falsa, sino en la confianza social en la posibilidad de distinguirla.

El sexto riesgo es la opacidad de responsabilidades en la cadena informativa. Mientras que en la propaganda tradicional es sencillo identificar la autoría, al contratante, el medio de difusión y el costo; en entornos digitales, la cadena puede involucrar consultores, agencias, plataformas, *influencers*, granjas de contenido, cuentas anónimas, herramientas automatizadas, servicios de empresas trasnacionales y pagos difíciles de rastrear. La atribución de responsabilidad se vuelve un reto.

El séptimo riesgo es la limitación de los remedios institucionales. Aquí algunos escenarios: una multa administrativa puede ser insuficiente frente a un contenido viral que afectó la campaña, una orden de retiro de contenido puede ser inocua ante la vertiginosa rapidez con la que este puede ser replicado en múltiples plataformas, una aclaración institucional puede no alcanzar a los públicos impactados por cierta falsedad propagada en redes sociales. Estos desafíos, entre otros más, obligan a pensar medidas cautelares, etiquetado, rectificaciones, trazabilidad, repositorios de publicidad, cooperación con plataformas y alfabetización digital.

El impacto democrático-electoral de la IA y las plataformas digitales no se mide solo por su capacidad de cambiar resultados. Se mide a su vez por la influencia en las condiciones del proceso electoral: la calidad de la información disponible, la equidad de la competencia, la autenticidad del debate, la seguridad de las candidaturas y grupos de atención prioritaria, la efectividad en los sistemas de fiscalización, la confianza en las autoridades, la integridad de la prueba y la legitimidad pública de la elección. La justicia electoral debe situarse en ese terreno. No le corresponde resolver todos los problemas de la esfera digital; ello debe ser resultado de una política pública de Estado. Sin embargo, sí le corresponde aportar criterios para los casos en que esos problemas afecten derechos político-electorales o principios constitucionales. Su tarea no es regular toda la tecnología, sino decidir cuándo una práctica digital cruza la frontera de la licitud electoral. Esa frontera no siempre es evidente. Exige distinguir, por ejemplo, la crítica de la calumnia, la sátira del engaño, la automatización legítima de la simulación, la segmentación ordinaria de la manipulación, el error de la desinformación deliberada, la propaganda marcada de violencia y la innovación del abuso.

Este volumen busca contribuir precisamente a esta tarea, bajo la premisa, entre otras, de que el debate en torno a la IA y las plataformas digitales en el terreno político-electoral no debe reducirse entre el apocalipsis tecnológico y el solucionismo tecnológico. Se trata, más bien, de la infraestructura de un nuevo poder comunicativo complejo que puede ampliar el ejercicio de derechos o restringirlos; distribuir mejor la información pública o fragmentar el debate; fortalecer la participación y representatividad ciudadana, o acentuar las desigualdades.

La IA y las plataformas digitales obligan a repensar la forma en que las democracias regulan aspectos como la comunicación política, la propaganda electoral y la integridad informativa, así como la responsabilidad de los actores públicos y privados. El reto no consiste solo en añadir nuevas prohibiciones a la legislación electoral. Exige construir una arquitectura normativa capaz de ordenar un ecosistema comunicativo dinámico, transnacional, técnicamente complejo y gobernado por empresas privadas cuya lógica principal es comercial.

La primera dificultad regulatoria para este propósito, en este contexto, es conceptual. Las categorías clásicas del derecho electoral fueron diseñadas para un entorno de la comunicación democrática enteramente distinto. Esto no significa que tales categorías tradicionales sean del todo obsoletas. El reto es que se reinventen acordes con estas nuevas condiciones tecnológicas de los procesos deliberativos y representativos. ¿Cómo traducir los principios básicos, constitutivos del régimen democrático, en un espacio en el que la propaganda es sintética, la autoría de los mensajes es difusa, la difusión del contenido es automatizada y el daño ocurre antes de la intervención de la autoridad? Sobra mencionar que esta interrogante plantea varios desafíos; a modo de ejemplo, aquí se apuntan algunos de ellos.

Un primer desafío consiste en distinguir entre los usos permitidos con entera libertad, aquellos que exijan cumplir ciertas obligaciones mínimas y, por supuesto, los enteramente prohibidos en campañas y procesos electorales. Esta clasificación por niveles de riesgo, con todos sus problemas de definición, se alinea mejor con la naturaleza de la tecnología que una prohibición general. Una regla amplia que prohíba toda IA en campañas sería poco viable, difícil de fiscalizar y potencialmente contraria a los usos legítimos de accesibilidad, eficiencia y comunicación. Una regla por entero permisiva, en cambio, dejaría sin respuesta los riesgos de suplantación, manipulación, opacidad y violencia. El derecho electoral debe construir criterios que atiendan la finalidad, el sujeto, el medio, la transparencia, el alcance, el daño potencial y el contexto.

Un segundo reto atañe a la transparencia: se requiere un andamiaje de mecanismos capaz de garantizar este principio en el entorno digital. De tal manera que, por ejemplo, los contenidos generados o alterados mediante IA que tengan finalidad electoral se identifiquen de manera visible cuando su carácter sintético pueda modificar la percepción ciudadana, o bien, que la publicidad política digital sea consultable por medio de repositorios que permitan conocer quién pagó el anuncio, a quién fue dirigido, durante cuánto tiempo circuló, cuánto costó y con qué criterios de segmentación se difundió.

Otro reto clave es la responsabilidad de las plataformas digitales. Las plataformas no son partidos políticos ni autoridades electorales; son empresas privadas trasnacionales; sin embargo, cumplen una función decisiva en la circulación de información pública; su diseño determina qué contenidos se ven, qué mensajes se amplifican, a quiénes llegan qué anuncios, qué materiales se retiran, qué cuentas se suspenden y qué prácticas se toleran. Ahora bien, la regulación democrática no puede ignorar ese poder privado. La pregunta obligatoria es: ¿cómo evitar que estos intermediarios en línea se conviertan en promotores o censores privados del debate público y, a su

vez, que el Estado intervenga de manera excesiva, en detrimento de la libertad de expresión, en estos espacios?

Un cuarto reto, de carácter probatorio, consiste en que la justicia electoral necesita criterios para valorar contenidos digitales cuya autenticidad puede ser discutida. Esto exige fortalecer capacidades técnicas sin abandonar las garantías procesales. La autoridad debe poder solicitar metadatos, analizar trazabilidad, ordenar peritajes, solicitar a las partes involucradas que identifiquen plenamente el uso de IA en su propaganda o mensajes y, en caso de que no lo hagan, revertir la carga de la prueba a las partes, valorar patrones de difusión, identificar indicios de coordinación y distinguir manipulación técnica de edición ordinaria. También debe reconocer los límites de la prueba técnica. No siempre será posible acreditar con certeza absoluta quién produjo un contenido o si fue generado por determinado modelo.

En esta línea es necesario repensar las medidas cautelares. En materia electoral, el tiempo es decisivo. Un contenido falso puede producir efectos antes de que termine el procedimiento sancionador. Por ello, las autoridades deben contar con mecanismos ágiles para preservar evidencia, ordenar el retiro o el etiquetado cuando exista riesgo grave, solicitar información a plataformas y evitar daños irreparables. Pero esa rapidez debe convivir con estándares estrictos para no restringir el discurso político legítimo. En ese sentido, la crítica, la sátira, el humor, la exageración retórica y la opinión dura tienen protección constitucional. La respuesta cautelar debe dirigirse a engaños materiales, suplantaciones, violencia, datos falsos sobre procedimientos electorales o afectaciones claras a derechos.

La lista de desafíos continúa, por supuesto. Entre ellos, resulta clave proteger datos personales, impedir el uso abusivo de información sensible, así como fiscalizar gastos digitales vinculados con segmentación, *bots*, contenido sintético, consultoría algorítmica o campañas de influencia. Además, otro reto es reconocer nuevas formas de violencia política digital —en especial en contra de mujeres, personas de la diversidad sexual, comunidades indígenas y otros grupos de atención prioritaria— a partir de los recursos que ofrecen para ello la IA y las plataformas digitales.

Ahora bien, la justicia electoral mexicana ya ha empezado a enfrentar varios de estos retos en casos concretos. El desarrollo de criterios judiciales, como se sabe, avanza de manera casuística. Este método tiene ventajas: permite prudencia, evita sobrerregulación y permite emitir criterios a partir de casos reales. Pero también tiene límites: puede llegar tarde, generar incertidumbre y cargar sobre el Tribunal decisiones que deberían tener una base legislativa o administrativa más clara. Por eso, tal vez

sea momento de pensar en una regulación que combine legislación, lineamientos administrativos y jurisprudencia.

La meta última, en cualquier caso, es clara: construir una democracia digitalmente informada, electoralmente íntegra y jurídicamente garantista. Una democracia en la que la tecnología pueda servir a la participación, pero no sustituir la deliberación; en la que la innovación no sea excusa para la opacidad; en la que la libertad de expresión no se utilice como protección para la falsedad ni la violencia; en la que la justicia electoral pueda actuar con rapidez sin perder rigor; en la que la ciudadanía cuente con herramientas para ejercer sus derechos en un espacio público cada vez más mediado por sistemas inteligentes.



Coordenadas jurídicas



La deliberación democrática contemporánea sufre una de sus transformaciones más profundas, a partir de la irrupción de las plataformas digitales y la inteligencia artificial (IA). Hoy la esfera pública habita en un ecosistema informativo definido por tecnologías digitales, plataformas privadas, sistemas automatizados de recomendación, modelos inteligentes que amplifican y distribuyen contenidos, gigantescas bases de datos y un largo etcétera. Las campañas electorales, y la diversidad de aspectos que confluyen en ellas, ciertamente se siguen desarrollando en medios tradicionales, con sus característicos mensajes dirigidos a un público masivo, sin posibilidad de interactuar con estos, y sometidos a criterios editoriales definidos y operados por humanos. Pero también tienen como escenario, y cada vez con más incidencia, plataformas digitales que curan el contenido de sus usuarios mediante algoritmos diseñados para una selección personalizada de la comunicación, y cuyos estándares comunitarios se operan en buena medida por sistemas automatizados.

Esta transformación obliga a repensar la justicia electoral desde una pregunta básica: ¿cómo preservar aspectos inherentes a la dinámica democrática como la libertad de expresión, la equidad de la contienda, la autenticidad del sufragio y el derecho a la información, cuando los mensajes políticos pueden generarse automáticamente, circular de manera segmentada entre la ciudadanía, así como recrear de manera verosímil voces y rostros falsos de personas?

La IA no inaugura cada uno de estos problemas; por el contrario, un reto perenne de la democracia moderna ha sido justo asegurar condiciones para una deliberación genuina a partir de información veraz. Pero, sin duda, los intensifica y complejiza, abarata y acelera la producción y difusión de contenido, reduce las barreras para manipular información y ofrece herramientas sin precedentes para ello. Asimismo dificulta establecer la cadena de responsabilidad respecto de la propagación intencionada de falsedades o la afectación de derechos, entre otras nuevas complejidades provenientes de viejas dificultades.

La cuestión, por supuesto, no consiste en prohibir la tecnología ni en celebrar acríticamente su incorporación, como ya se ha apuntado. El desafío democrático está, más bien, en construir criterios institucionales capaces de distinguir entre usos legítimos, innovadores e incluso útiles de la IA y, por el contrario, usos que lesionan derechos, distorsionan la competencia democrática y deterioran la confianza pública. En esa línea, la justicia electoral debe desarrollar capacidades para comprender este entorno tecnológico en el que ocurren las infracciones, exigir trazabilidad de las conductas y determinar responsabilidades, valorar evidencia digital, ordenar remedios oportunos y comunicar sus decisiones de manera clara en términos jurídicos, pero también tecnológicos y, por supuesto, pedagógicos, con un enfoque ciudadano.

Derivado de lo anterior, el presente texto propone un planteamiento de las diversas aristas de esta discusión en el ámbito político-electoral, a partir del andamiaje constitucional, legal y jurisdiccional del país. Y, para ello, este se organiza en seis ejes clave: 1) el impacto de la tecnología y la IA en la labor jurisdiccional electoral; 2) los límites aplicables a la propaganda política generada mediante IA; 3) el alcance del control jurisdiccional sobre plataformas digitales privadas; 4) la posibilidad de sancionar la desinformación intencionada mediante una adaptación de la doctrina de la real malicia; 5) los efectos de la microsegmentación política en la igualdad de la contienda, y 6) las capacidades institucionales que requiere el Estado mexicano para enfrentar la manipulación digital del voto.

Inteligencia artificial y la función jurisdiccional electoral

Aunque el origen de la expresión "inteligencia artificial" se ubica en la famosa Conferencia de Dartmouth University (1956), para su desarrollo fue necesario esperar la llegada de, por lo menos, dos factores clave: la consolidación del mundo en línea a partir de internet, con su correspondiente digitalización de enormes cantidades de información, y la evolución de la tecnología de los microprocesadores que determina el poder de cómputo para procesar tal cantidad de información. De tal manera que, con la llegada del siglo XXI, fue posible por fin contar con sistemas informáticos de un impacto social masivo, capaces de realizar actividades comparables a las de la mente humana, tales como el aprendizaje, el razonamiento lógico y la toma de decisiones a partir de cierta información y una serie de metas previamente establecidas.

La definición técnica de la IA ha cambiado desde mediados del siglo pasado y, como suele suceder, está abierta a un permanente debate entre especialistas. Se ha

descrito, por ejemplo, como la capacidad de una máquina para desempeñar tareas que normalmente requerirían inteligencia humana, mediante el análisis de datos, el aprendizaje de patrones y la producción de inferencias o decisiones guiadas por objetivos (International Organization for Standardization, 2026). Por su parte, instituciones y empresas —como Google Cloud, la Organización de las Naciones Unidas, la National Aeronautics and Space Administration (NASA) y Microsoft— han definido la IA como una tecnología transversal que incide en informática, datos, productividad, educación, ciencias sociales, reconocimiento de imágenes, asistentes virtuales y toma de decisiones automatizada (Microsoft, 2026a; National Aeronautics and Space Administration, 2026; Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 2026).

El trabajo de Stuart Russell y Peter Norvig, dos de los referentes más relevantes en el campo de la inteligencia artificial en el ámbito internacional, ha sido central en la consolidación conceptual, al concebirla como el estudio de agentes que perciben su entorno y actúan sobre él. Su enfoque no reduce la IA a la imitación de conductas humanas, sino que la asocia con la acción racional, el aprendizaje y la adaptación (Russell y Norvig, 2020). De ahí que la discusión contemporánea incorpore dimensiones de ética, seguridad, equidad y alineación de objetivos con valores humanos. Una última definición: como se mencionó, la expansión del acceso al uso de la IA no se puede entender sin las plataformas de IA, entendidas como un entorno unificado e integral para diseñar, personalizar y gestionar soluciones mediante la IA (Microsoft, 2026b).

En este sentido, además de los sistemas inteligentes de moderación y distribución de contenidos de intermediarios como Facebook, Instagram y TikTok, también existen herramientas generativas y *chatbots* como ChatGPT, Copilot, Gemini o Claude; aplicaciones de productividad y trabajo, tales como Notion AI, Grammarly u Otter; asistentes de programación como GitHub Copilot o Cursor; servicios de video, voz y conocimiento empresarial, como Synthesia, ElevenLabs, Watsonx o Vertex AI, y plataformas de investigación como Semantic Scholar, Scite o SciSpace.

Ahora bien, para comprender el impacto jurídico de la IA, es necesario distinguir entre algunas de sus principales ramificaciones: *machine learning*, aprendizaje profundo e IA generativa. El aprendizaje automático permite que los modelos identifiquen patrones en datos y realicen inferencias sobre información nueva, lo cual habilita condiciones para una mejor toma de decisiones en ámbitos que van desde la logística de transporte terrestre, aéreo y marítimo hasta la medicina y el diagnóstico de enfermedades como el cáncer. El aprendizaje profundo utiliza redes neuronales con múltiples capas para el reconocimiento de imágenes o el procesamiento del lenguaje natural. Por último,

la IA generativa permite crear textos, imágenes, audios o videos originales a partir de modelos entrenados con grandes cantidades de información. Esta última es la que más intensifica los riesgos electorales contemporáneos, porque puede producir de manera rápida y creíble contenidos que antes requerían equipos especializados.

La función jurisdiccional electoral, entonces, ha transitado de un entorno tradicional y analógico hacia uno digital y automatizado. El impacto de esta transformación en la justicia electoral se debe analizar a partir de una doble perspectiva: interna y externa.

En la primera, el Tribunal Electoral del Poder Judicial de la Federación (TEPJF) ha desarrollado herramientas como el juicio en línea y el asistente virtual Alfonsina. El juicio en línea permite promover, sustanciar y resolver medios de impugnación de manera digital, ampliando el acceso a la justicia en contextos tecnológicos contemporáneos. Alfonsina permite que cualquier persona pueda consultar precedentes, jurisprudencia, transparencia y archivos mediante lenguaje coloquial, sin requerir conocimientos especializados.

Este proceso de incorporación tecnológica también comprende el uso de herramientas privadas de IA generativa, como Copilot de Microsoft, que forma parte del ecosistema institucional de apoyo al trabajo jurídico: redacción, sistematización, consulta preliminar y organización de información, en un contexto de capacitación institucional y colaboración con proveedores tecnológicos (El Heraldo, 2025). Sin embargo, estas herramientas no pueden sustituir la decisión judicial. La sentencia debe seguir siendo humana, motivada, responsable y atribuible a una persona. El verdadero riesgo no es que la IA apoye tareas administrativas o analíticas, sino que desplace la responsabilidad que corresponde a las personas juzgadoras.

La perspectiva externa, por su parte, se relaciona con el uso de tecnología por parte de actores políticos, partidos, candidaturas, simpatizantes, *influencers*, plataformas o redes coordinadas. Antes, la propaganda político-electoral, por ejemplo, se difundía principalmente en radio, televisión, impresos y espectaculares, es decir, medios de comunicación identificables, con un sistema de difusión centralizado y masivo y con criterios editoriales verificables por humanos. Las autoridades podían conocer al emisor, constatar el contenido y razonar probatoriamente a partir de documentos, grabaciones o constancias físicas. En cambio, el entorno digital multiplica emisores, disocia la autoría y la difusión, fragmenta audiencias y genera contenidos efímeros por la dinámica de propagación de información.

Ante este cambio, en una primera etapa, los tribunales electorales enfrentaron problemas vinculados con internet y redes sociales: propaganda en Facebook o Twitter, mensajes de texto, páginas web y videos alojados en plataformas. El contenido era

producido mayoritariamente por personas que difundían sus mensajes mediante estos intermediarios en línea. La discusión giraba en torno a la posibilidad de identificar a los usuarios, atribuir responsabilidades y valorar pruebas técnicas. Hoy, sin embargo, con la IA generativa, el problema se profundiza: no solo es difícil ubicar quién difundió un mensaje, sino también determinar si el contenido en cuestión es auténtico, sintético o manipulado.

La democracia se está desplazando, como ya se ha apuntado, a plataformas digitales privadas y globales, mediadas por algoritmos que organizan información, priorizan contenidos, clasifican audiencias y amplifican mensajes. La tecnología no es neutra: decide qué se ve, qué se oculta, qué se recomienda y qué se viraliza. En materia electoral, esto se traduce en microsegmentación política, propaganda focalizada, uso de *influencers,* contenido sintético, desinformación, *astroturfing* y *deepfakes*.

Los desafíos probatorios son especialmente relevantes aquí; la autenticidad del contenido se vuelve incierta porque no existe un método infalible para determinar si un audio, una imagen o un video fue generado o modificado mediante IA (Heaton *et al*., 2026). Es decir, incluso la misma IA no ofrece una prueba infalible de si cierto contenido es falso o manipulado o, al menos, no acorde con las exigencias de los tiempos procesales de la justicia electoral. La atribución de responsabilidad se complica porque intervienen herramientas tecnológicas diversas, plataformas, algoritmos de difusión, usuarios de buena fe y también otros que, aprovechando las herramientas de la IA y la operación de las redes sociales, articulan estrategias para desinformar. Los esquemas clásicos de prueba documental o pericial resultan insuficientes frente a estos sistemas (Organización para la Cooperación y el Desarrollo Económicos, 2024).

Por ejemplo, un precedente significativo es la sentencia SUP-REP-893/2024 y acumulados (2024), relativa al uso de imágenes de niñas, niños y adolescentes generadas o modificadas mediante IA en propaganda electoral. El caso muestra una justicia electoral que empieza a actuar preventivamente frente a riesgos digitales, aunque sin perder de vista la tipicidad de la conducta y la necesidad de proteger derechos humanos en entornos tecnológicos muy cambiantes.

La experiencia comparada ofrece referentes útiles. La Unión Europea ha avanzado en obligaciones de transparencia y etiquetado de publicidad política y contenidos manipulados mediante IA, a partir de la Ley de Inteligencia Artificial de la Unión Europea (2024) y del Reglamento 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política (2024). Por ejemplo, Brasil ha adoptado reglas restrictivas sobre propaganda elaborada con IA en periodos cercanos a la jornada electoral (Swissinfo, 2026). Singapur, por su parte,

ha regulado la representación falsa de candidaturas mediante contenido sintético, con su Ley de Elecciones (Integridad de la Publicidad en Línea, 2024). Estos modelos no deben trasladarse mecánicamente, pero permiten pensar en respuestas que reduzcan obstáculos probatorios y faciliten la identificación de autoría y la trazabilidad.

En México, los Lineamientos y Principios para el Desarrollo Estratégico y Uso Regulado de la Inteligencia Artificial del Instituto Nacional Electoral (INE) constituyen una referencia institucional relevante (Acuerdo INE/JGE175/2025, 2025). Su principio central es el carácter auxiliar de la IA: no debe sustituir decisiones institucionales y debe operar con supervisión humana significativa. Además, incorporan legalidad digital, transparencia, explicabilidad algorítmica, trazabilidad, protección de datos personales, no discriminación y equidad tecnológica.

Propaganda política e inteligencia artificial

La segunda cuestión consiste en definir qué límites deben aplicarse a la propaganda política generada mediante IA. La pregunta ya no es si la IA debe existir en procesos electorales. Esa etapa quedó superada. El problema consiste en determinar qué reglas permiten que esta tecnología sea compatible con criterios que han dado forma a la conversación pública democrática, tales como la veracidad de la información, la distinción entre hechos y opiniones y la línea entre expresiones y violencia, y evitar que se convierta en una ventaja para quien mejor engaña o simula.

Vale la pena insistir en que el impacto de la IA en la esfera político-electoral no crea por sí solo un problema normativo inédito. Más bien, intensifica y complejiza riesgos ya conocidos: suplantación de identidad; manipulación informativa; afectaciones al honor; calumnia; vulneración de derechos de niñas, niños y adolescentes; propaganda encubierta, y distorsión del debate público. Lo novedoso, sin embargo, es que estos riesgos se gestan ahora en un escenario regido por una nueva escala de propagación, velocidad y aparente verosimilitud.

La propaganda generada con IA puede adoptar múltiples formas: imágenes de personas inexistentes, audios clonados, *deepfakes*, avatares, rostros sintéticos, voces artificiales, mensajes automatizados, *bots* conversacionales o textos personalizados. Esta capacidad altera una premisa básica del debate público de la democracia moderna y del surgimiento de la radio y la televisión: que la evidencia audiovisual conserva una relación mínima con la realidad.

En México no existe todavía un marco integral de regulación electoral de la IA. Hay iniciativas legislativas, como la propuesta de Ley Federal que Regula la Inteligencia Artificial (2024), orientadas a establecer principios generales de desarrollo y uso responsable. Pero la respuesta electoral ha sido, hasta ahora, casuística, por medio de precedentes jurisdiccionales, reglas administrativas específicas y criterios interpretativos.

El caso SUP-REP-893/2024 y SUP-REP-900/2024 (2024), como se apuntó, marcó un punto de partida. La Sala Superior determinó que, en el asunto concreto, no se actualizó una vulneración al interés superior de la niñez por el uso de una imagen infantil generada con IA, al considerar que no correspondía a una persona real identificable. Sin embargo, vinculó al INE para ajustar lineamientos e implementar mecanismos de verificación respecto del uso de imágenes generadas, editadas o modificadas mediante IA en propaganda político-electoral.

A partir de esa vinculación, el INE emitió reglas para la protección de niñas, niños y adolescentes en propaganda y mensajes electorales del Proceso Electoral Extraordinario del Poder Judicial de la Federación 2024-2025 (Instituto Nacional Electoral, 2025). Las reglas obligan a insertar cintillos o leyendas cuando se utilicen imágenes, voces o datos de niñas, niños o adolescentes generados o editados con IA; conservar documentación sobre la herramienta utilizada, el método, la fecha y las etapas de creación, y acreditar, cuando sea necesario, la información que permita verificar la licitud del uso.

Los precedentes posteriores muestran la complejidad del estándar. En el expediente SRE-PSL-19/2025 (2025) se denunció el uso de imágenes de personas menores de edad presuntamente creadas mediante IA en una publicación de Facebook de una candidatura judicial. La entonces Sala Regional Especializada concluyó que no había vulneración al interés superior de la niñez porque las imágenes eran generadas artificialmente y no correspondían a personas reales identificables. En contraste, en la sentencia SRE-PSD-15/2025 (2025), al no acreditarse que las imágenes fueran sintéticas, se consideró actualizada la vulneración por la aparición de personas menores de edad reales sin consentimiento ni cumplimiento de los lineamientos.

De estos casos se desprende una regla práctica: la IA no elimina los deberes de cuidado; los desplaza hacia la verificación. Cuando una imagen es real e identificable, subsisten los requisitos reforzados de protección. Cuando es sintética, debe existir transparencia suficiente para acreditar su origen y evitar confusión. La autoridad no debe sancionar sin tipicidad, pero sí puede exigir documentación que reduzca la incertidumbre.

La frontera democrática puede formularse así: la propaganda puede persuadir, criticar y simplificar, pero no debe suplantar identidades, fabricar hechos,

atribuir declaraciones falsas o engañar materialmente al electorado. La libertad de expresión protege la crítica dura y el discurso político confrontativo, pero no exige tolerar la falsificación audiovisual dirigida a manipular condiciones básicas de información.

Un modelo normativo razonable debe combinar transparencia, etiquetado, trazabilidad, prohibición focalizada de la suplantación y remedios rápidos con una revisión posterior. Toda propaganda política generada, total o parcialmente, mediante IA debería ser claramente identificable para la ciudadanía. Debe prohibirse clonar la voz, la imagen o los gestos de personas reales sin consentimiento, atribuir declaraciones falsas, simular interacción humana mediante *bots* o utilizar datos personales sensibles para manipular decisiones electorales.

Las reglas también deben ser temporales y contextuales. Durante las campañas, los periodos de reflexión y la jornada electoral, la velocidad de circulación de contenidos exige límites reforzados y procedimientos expeditos. La asimetría entre la velocidad de la mentira y el tiempo de la verificación constituye el núcleo del problema democrático contemporáneo. Si la respuesta institucional llega después de que el contenido se haya viralizado, el remedio puede ser jurídicamente correcto, pero social y políticamente irrelevante.

El objetivo no es regular mensajes en abstracto, sino proteger la confianza pública como bien democrático. Cuando una sociedad no comparte un mínimo de realidad verificable, la dinámica democrática deja de ser un espacio deliberativo y se convierte en una mera guerra de percepciones subjetivas. Por eso, regular la propaganda con IA no significa censurar la creatividad tecnológica, sino preservar las condiciones para que la libertad de elección siga siendo auténtica.

Plataformas digitales privadas y control jurisdiccional

El tercer eje aborda el alcance del control jurisdiccional respecto de las plataformas digitales privadas en los procesos electorales. Aquí es indispensable partir de un dato fundamental: el acceso a internet en México sigue creciendo; con todas las asignaturas aún pendientes en ciertas regiones del país, la brecha digital se reduce cada vez más. En 2024, 83.1 % de la población, equivalente a 100.2 millones de personas, usaban internet; la conectividad era mayor en las zonas urbanas que en las rurales, y el teléfono móvil era el principal medio de acceso (Reglas para la Protección de Niñas,

Niños y Adolescentes en Materia de Propaganda y Mensajes Electorales para el Proceso Electoral Extraordinario, 2025).

El actual modelo mexicano de comunicación político-electoral fue diseñado principalmente para radio y televisión. La reforma electoral de 2007-2008 estableció la prohibición de la contratación privada de propaganda político-electoral en esos medios, la administración exclusiva de los tiempos del Estado por la autoridad electoral y la asignación gratuita y equitativa de tiempos a partidos y candidaturas (Valdés, 2022). Su finalidad era impedir que el poder económico determinara el acceso a los medios masivos tradicionales.

Ese modelo no previó de manera expresa internet ni las plataformas digitales, ni mucho menos los riesgos de la IA generativa. De ahí que exista una asimetría regulatoria entre medios tradicionales, fuertemente regulados, y las plataformas digitales, en las que sí es posible contratar publicidad política, segmentar audiencias, aprovechar la resonancia de *influencers* (con la línea gris que implica su participación entre la libertad de expresión y la propaganda), promover contenidos y generar mensajes diferenciados sin un control equivalente al de la radio y la televisión (Artículo 19, 2024).

Al poco tiempo de que se aprobara este modelo de comunicación político-electoral, la jurisprudencia electoral tuvo que enfrentar este desfase entre un nuevo esquema regulatorio y la irrupción de la comunicación política *plataformizada* que no se contempló en el primero.

En el SUP-RAP-153/2009 (2009), relativo a un video difundido en YouTube contra el gobernador de Veracruz, la Sala Superior confirmó la dificultad para atribuir responsabilidad por contenidos alojados en una red global sin un banco de datos centralizado. En el SUP-RAP-41/2012 (2012), relativo a la promoción del candidato presidencial Enrique Peña Nieto en internet, se destacó nuevamente la dificultad procesal para atribuir contenidos de páginas web al actor político denunciado.

El modelo, no obstante, se adaptó con el tiempo, caso por caso, desde la arena judicial. En el SUP-REP-542/2015 y SUP-REP-544/2015 acumulados (2015), la Sala Superior confirmó sanciones al Partido Verde Ecologista de México (PVEM) por una estrategia propagandística en Twitter durante la veda electoral mediante personas famosas. En el SUP-RAP-172/2021 (2021), confirmó una multa al PVEM por mensajes de *influencers* en la plataforma Instagram durante la veda. Estos precedentes muestran que las redes sociales no están fuera del derecho electoral: la dificultad radica en probar la coordinación, el financiamiento, el beneficio, la autoría y el contexto.

El control jurisdiccional respecto de las plataformas digitales es, por ahora, indirecto, casuístico y reactivo. No recae de manera general en la plataforma como sujeto regulado, sino sobre el contenido difundido, la conducta del emisor y el impacto del mensaje en el proceso electoral (Valdés, 2022). Las plataformas funcionan como medio comisivo o como infraestructura de difusión; las autoridades jurisdiccionales intervienen cuando existe un procedimiento o medio de impugnación que vincula la conducta de sus usuarios a una posible vulneración de los principios electorales.

Esta arquitectura es insuficiente. Las plataformas, si bien son privadas, administran espacios que cumplen funciones públicas deliberativas. Sus reglas internas, algoritmos, bibliotecas de anuncios, sistemas de recomendación, políticas de retiro y mecanismos de verificación inciden en la conversación democrática. Es más, sus estándares comunitarios, que definen qué tipo de expresiones pueden circular en ellas, no siempre están acordes a la libertad de expresión establecida en la Constitución mexicana y en los precedentes judiciales correspondientes.

En efecto, el diseño actual de internet parte del supuesto de que los intermediarios en línea gozan de inmunidad respecto del contenido de sus usuarios. El origen de esta protección legal se encuentra en el derecho estadounidense, en la sección 230 de la Communications Decency Act de 1996. Su lógica consistió en proteger a los intermediarios en línea frente a la responsabilidad jurídica por los contenidos publicados por sus usuarios, al tiempo que se les permitió moderar, retirar o restringir contenidos ofensivos o dañinos sin que esa intervención los convirtiera automáticamente en responsables editoriales.

En México, esa protección ingresó al orden jurídico principalmente por la vía del Tratado entre México, Estados Unidos de América y Canadá (2020), mediante el artículo 19.17 acerca de los servicios informáticos interactivos. Dicha disposición impide que los Estados parte traten a los proveedores de estos servicios como responsables del contenido generado por terceros. El anexo 19-A introdujo, además, matices relevantes para México: reconoció que esta regla debía armonizarse con los artículos 6.º y 7.º constitucionales, relativos a la libertad de expresión y la difusión de ideas, y dejó abierta la posibilidad de interpretar ciertas excepciones conforme a criterios de orden y moral públicos previstos en el propio tratado.

Sin embargo, conviene distinguir entre inmunidad y responsabilidad limitada. La inmunidad supone una protección fuerte frente a demandas por contenidos de terceros: la plataforma no responde, en principio, por lo que publican sus usuarios. La responsabilidad limitada, en cambio, admite un modelo más condicionado: la

plataforma conserva protección jurídica solo si cumple ciertos deberes mínimos de buena fe, transparencia, diligencia, moderación razonable o cooperación institucional. Desde esta segunda lectura, el debate no sería si las plataformas deben responder por todo, sino en qué condiciones pueden conservar su protección legal cuando su inacción, sus sistemas de moderación o sus algoritmos contribuyen a daños relevantes en la conversación pública y en los procesos electorales.

Lo cierto es que, hasta ahora, ni la Suprema Corte de Justicia de la Nación ni el TEPJF han tenido oportunidad de emitir un criterio de fondo acerca del alcance constitucional o electoral de esta inmunidad derivada del T-MEC. Existen discusiones judiciales y electorales en torno a la libertad de expresión en internet, redes sociales, propaganda digital, violencia política o moderación de contenidos, pero todavía no existe un pronunciamiento específico que defina si el artículo 19.17 debe entenderse en México como una inmunidad amplia, como una responsabilidad limitada condicionada por deberes de buena fe o como una protección sujeta a excepciones cuando estén comprometidos los derechos fundamentales, la integridad electoral o el orden público democrático.

Así, la discusión debe evitar dos extremos. El primero es considerar a las plataformas simples intermediarias neutrales, sin responsabilidad frente a procesos democráticos. El segundo es imponerles deberes estatales de censura o control de contenidos incompatibles con la libertad de expresión. La solución razonable es una regulación basada en deberes de diligencia, la transparencia, la cooperación, la preservación de evidencia, los repositorios de publicidad política y los mecanismos de respuesta rápida frente a riesgos electorales.

La experiencia comparada ofrece referentes en esta dirección. Brasil (Ley Electoral n.º 9.504/1997, 1997; Resolución TSE n.º 23.610/2019, 2019) ha celebrado acuerdos de colaboración con las plataformas para la verificación prioritaria de cuentas de candidaturas, retiro de contenidos falsos y la entrega de datos acerca de las publicaciones virales con contenido electoral. Canadá (Elections Modernization Act, 2019) exige repositorios públicos de anuncios políticos. Estados Unidos ha recurrido de manera fragmentaria a políticas privadas de plataformas ante la falta de aprobación de la Honest Ads Act (2023). Estos modelos muestran que la autorregulación puede ser útil como etapa transitoria, pero no sustituye un marco normativo estable.

El principio de equidad en la contienda debe seguir siendo el eje rector. La intervención estatal o la cooperación con plataformas se justifican no por una lógica de control del pensamiento, sino por la necesidad de evitar que la opacidad digital

permita distorsionar impunemente. La regulación debe preservar la libertad de expresión y, al mismo tiempo, asegurar la certeza, la trazabilidad, la identificación de propaganda pagada, la transparencia en la segmentación y la protección del voto informado.

En síntesis, el alcance del control jurisdiccional no debe imaginarse como un poder general sobre las plataformas, sino como un conjunto de herramientas para revisar conductas concretas, exigir colaboración, valorar evidencia y ordenar medidas cuando el uso de plataformas comprometa bienes constitucionales. La reforma de fondo, sin embargo, corresponde al legislador y a las autoridades administrativas con capacidad reglamentaria.

Desinformación intencionada, real malicia y libertad de expresión digital

La desinformación es un fenómeno cuyas consecuencias no se limitan al plano comunicativo y periodístico; también adquiere una dimensión jurídico-electoral cuando incide en aspectos como la equidad de la contienda, el derecho a la información libre de interferencias, la formación libre de la voluntad ciudadana, así como la autenticidad del sufragio. El problema se vuelve más grave cuando la falsedad deja de ser un error aislado y se convierte en estrategia deliberada, coordinada y amplificada por dinámicas algorítmicas que premian la emoción y la interacción por encima de la veracidad.

La IA generativa, ahora de acceso masivo mediante múltiples plataformas digitales, reduce las barreras de entrada a herramientas que pueden ser usadas para generar desinformación y, en ese sentido, incrementa la capacidad de producción de contenidos maliciosos. Casos como Team Jorge —nombre de un equipo de contratistas dedicados a actividades ilegales en el mundo digital como piratería, hackeo y campañas de propagación de falsedades para manipular comportamientos electorales— ilustran la existencia de mercados dedicados a producir y distribuir campañas de desinformación. En este sentido, durante 2024 circularon en México narrativas falsas sobre supuestos planes de gobierno, como el cierre de la Basílica de Guadalupe o la abolición de la propiedad privada. La sofisticación técnica no siempre es necesaria, pero la IA aumenta la escala y la credibilidad del engaño (Pozo y Rojas, 2024).

La libertad de expresión es un derecho preferente en materia electoral. Protege a quien emite ideas y también el derecho social de recibir información plural.

El debate electoral debe ser robusto, crítico e incluso incómodo. El estándar no es el discurso cortés, sino un debate político intenso compatible con la deliberación democrática. Por ello, cualquier intervención estatal debe evitar convertirse en censura directa o indirecta.

El derecho electoral mexicano, sin embargo, reconoce fronteras. La calumnia electoral, entendida como imputación de hechos o delitos falsos con impacto electoral, constituye un límite a la libertad de expresión. En redes sociales, el TEPJF ha sostenido una presunción de espontaneidad del discurso ciudadano, pero también ha exigido valorar la calidad de la persona emisora y el contexto del mensaje. La jurisprudencia 13/2024 (2024) ordena tomar en cuenta la calidad de la persona emisora y el entorno en el que se emite un mensaje para acreditar infracciones en redes sociales.

La pregunta es si la doctrina de la real malicia puede utilizarse para sancionar la desinformación intencionada. La real malicia exige acreditar conocimiento de la falsedad o despreocupación temeraria respecto de la verdad. Su utilidad radica en que no sanciona lo falso sin más, sino la falsedad difundida con dolo o temeridad. Así, protege el error razonable, la crítica política y el periodismo de investigación y evita un efecto inhibidor en el debate público.

Una adaptación electoral de este estándar sería viable solo con condiciones estrictas. Primero, debe tratarse de un hecho verificable como falso, no de una opinión o juicio de valor. Segundo, debe acreditarse conocimiento de la falsedad o despreocupación temeraria por ella. Tercero, debe demostrarse atribución de autoría, coordinación o financiamiento, particularmente difícil en internet. Cuarto, debe existir un umbral de incidencia electoral: potencial real de afectar equidad, voto informado o autenticidad, más allá de molestias o crítica dura.

El estándar enfrenta límites. La carga probatoria es elevada; la atribución en entornos digitales es compleja por el anonimato, las cuentas apócrifas y la opacidad de la publicidad segmentada, y los procesos electorales exigen respuestas rápidas. La construcción probatoria de la real malicia puede tomar tiempo mediante peritajes, trazabilidad y análisis de contexto, mientras el daño informativo se consolida en horas. Por ello, la real malicia no basta por sí sola.

La respuesta debe combinar la responsabilidad ulterior excepcional con medidas no punitivas y preventivas: rectificaciones, etiquetas, desmentidos, información verificada, preservación de evidencia y procedimientos de retiro urgente cuando exista suplantación o falsedad material con riesgo electoral. La sanción debe ser la última respuesta y operar con legalidad estricta, tipicidad y proporcionalidad.

La desinformación deliberada, en suma, puede ser jurídicamente concebible como materia sancionable cuando se acredite malicia efectiva, falsedad verificable, atribución e incidencia electoral. Pero el estándar debe utilizarse de manera excepcional y focalizada. Su finalidad no es castigar el error ni moderar el tono del debate, sino proteger la integridad electoral frente a estrategias de falsificación material y manipulación del voto.

Microsegmentación del discurso político e igualdad en la contienda electoral

La microsegmentación es una de las transformaciones más relevantes del discurso electoral digital. Consiste en utilizar datos personales, perfiles conductuales, inferencias psicológicas, ubicación, historial de navegación, consumo, intereses y comportamiento en línea para dirigir mensajes políticos diferenciados a audiencias específicas. Esto es resultado de la irrupción de las plataformas digitales y del paso de los medios de comunicación de masas a las plataformas digitales. Su lógica es pasar de la propaganda pública general al mensaje invisible, personalizado y difícilmente fiscalizable.

La discusión acerca de la microsegmentación debe partir de un hecho: los algoritmos no son neutrales. Estos pueden producir o amplificar decisiones racializadas, clasistas o sexistas (Matsumi y Solove, 2025; Noble, 2018; Okidegbe, 2025). Además, la acumulación masiva de datos permite formas de vigilancia y predicción que transforman el vínculo entre ciudadanía, campañas y poder político (Rubinstein, 2014). La literatura ha advertido tanto promesas como amenazas de la publicidad política microdirigida para la democracia (Zuiderveen *et al*., 2018).

La microsegmentación, por supuesto, puede tener usos legítimos, pues permite que candidaturas comuniquen propuestas concretas a grupos interesados, reduzcan costos de campaña, identifiquen necesidades locales y acerquen información específica. Sin embargo, sus riesgos aparecen cuando se utilizan datos sensibles o inferidos del comportamiento de las personas, cuando los mensajes son opacos para el resto de la ciudadanía, cuando se envían mensajes contradictorios a audiencias distintas o cuando se busca desmovilizar selectivamente a grupos vulnerables.

El problema constitucional se centra en la igualdad de la contienda. Tradicionalmente, la equidad electoral se ha pensado en términos de dinero, acceso a medios y tiempo en radio y televisión. En el entorno digital, debe pensarse también en términos

de datos, capacidad analítica, poder de segmentación, infraestructura tecnológica y acceso a algoritmos de optimización. Quien cuenta con más datos y mejores herramientas puede hablar de manera distinta a cada votante, sin escrutinio público.

La literatura reciente advierte que el llamado *microtargeting* puede afectar la autonomía del voto, la deliberación común y la transparencia. Puede diseñarse un "traje a la medida" para influir emocionalmente en personas específicas (Cebrián, 2024). También puede causar un doble daño al electorado: manipular preferencias individuales y degradar el discurso público compartido (Bayer, 2020). En campañas contemporáneas, los comités de acción política y otros actores pueden financiar anuncios segmentados que no son visibles para quienes deberían fiscalizarlos democráticamente (Davis, 2025).

La privacidad electoral adquiere aquí una dimensión propia. Las campañas pueden usar datos obtenidos por parte de intermediarios (*brokers*), conglomerados empresariales, plataformas o interacciones digitales para clasificar votantes y adaptar mensajes (Klosowski, 2024). Casos como Cambridge Analytica, campañas de desmovilización selectiva o mensajes contradictorios según la audiencia demuestran que la microsegmentación no solo persuade; también puede inducir abstención, miedo, polarización o desconfianza selectiva (Channel 4 News, 2020). El daño democrático no siempre es visible. A diferencia de un *spot* televisivo, un anuncio segmentado puede aparecer solo por unas horas ante públicos reducidos y después desaparecer. Puede difundirse por WhatsApp o mensajería cerrada, fuera del radar institucional, y puede ajustar mensajes en tiempo real mediante IA. Esto dificulta la fiscalización, acreditación de pruebas, contradicción pública y, por lo mismo, control jurisdiccional.

Diversos estudios han mostrado que la ciudadanía muchas veces no advierte plenamente que está siendo microdirigida, lo cual debilita su capacidad de resistencia crítica (Noetzel *et al*. 2024). Otros han conceptualizado este fenómeno dentro del capitalismo de vigilancia, en el cual la extracción de datos conductuales se convierte en fuente de poder económico y político (Saura, 2023; Zuboff, 2019). La democracia enfrenta así el riesgo de que la persuasión electoral se base menos en argumentos públicos y más en explotación de vulnerabilidades.

Las respuestas regulatorias no deben prohibir toda segmentación. Una prohibición total sería difícil de aplicar y podría afectar formas legítimas de comunicación política que permite este nuevo escenario de IA y plataformas. Pero sí debe prohibirse el uso de datos sensibles sin consentimiento, exigir transparencia sobre criterios de segmentación, obligar a repositorios públicos de anuncios, limitar la publicidad política oscura, identificar patrocinadores y permitir auditorías. En ese sentido, International

Institute for Democracy and Electoral Assistance ha insistido en la necesidad de regular la publicidad política en línea y la microsegmentación desde una perspectiva legal, ética, política y tecnológica (International Institute for Democracy and Electoral Assistance, 2020).

Para el derecho electoral mexicano, la microsegmentación obliga a ampliar la noción de equidad. No basta revisar montos de gasto o acceso a medios. Debe analizarse, además, la ventaja derivada del uso de datos, algoritmos y opacidad. La pregunta central es si puede existir debate público genuino cuando una parte importante de la propaganda electoral es invisible para la mayoría de la ciudadanía. La respuesta requiere reglas de transparencia, capacidades técnicas y una cultura cívica capaz de reconocer la persuasión personalizada.

Capacidades institucionales versus manipulación digital del voto

La manipulación digital del voto puede definirse como la interferencia en las condiciones de información, deliberación y autonomía bajo las cuales la ciudadanía forma su decisión política, mediante los fenómenos que se han descrito en este texto a partir de las herramientas de la IA y las plataformas digitales. No se limita a manipular urnas o sistemas de cómputo; afecta el proceso de formación de la propia voluntad democrática.

Ante este riesgo, el Estado mexicano cuenta con capacidades electorales relevantes: un modelo normativo de propaganda, autoridades administrativas especializadas, órganos jurisdiccionales, procedimientos sancionadores, fiscalización, monitoreo de medios y experiencia en organización electoral. Sin embargo, esas capacidades fueron diseñadas para entornos analógicos o, en su caso, digitales, pero menos complejos. Hoy, por tanto, resultan insuficientes frente a la profundidad del alcance tecnológico de la IA. Esta interrogante, vale subrayar, no es menor: ¿cómo rediseñar las capacidades estatales para enfrentar estos desafíos? Ese es el punto neurálgico de una de las discusiones cuyas conclusiones definirán el futuro del régimen político.

La primera capacidad necesaria es regulatoria. El Estado debe diseñar reglas basadas en riesgos, no solo en herramientas. No toda IA debe regularse igual. La regulación debe distinguir entre contenido lícito, sintético transparente y engañoso, suplantación, manipulación, uso de datos sensibles y operaciones coordinadas. También debe prever

obligaciones diferenciadas para partidos, candidaturas, servidores públicos, plataformas, intermediarios e *influencers*.

En segundo lugar, es indispensable fortalecer la competencia técnica y pericial. Las autoridades electorales y jurisdiccionales requieren unidades permanentes capaces de analizar algoritmos, detectar *deepfakes*, auditar publicidad digital, preservar evidencia, identificar redes coordinadas, evaluar metadatos, comprender dinámicas de plataformas y realizar verificaciones forenses. La evidencia digital debe tratarse con protocolos de cadena de custodia, preservación y valoración adecuados.

Luego, es clave una capacidad de gobernanza interinstitucional. La manipulación digital del voto no puede enfrentarse por una sola autoridad. Requiere coordinación entre el INE, el TEPJF, los organismos públicos locales electorales, los tribunales locales, las autoridades de protección de datos personales, las instancias de ciberseguridad, las fiscalías electorales, las universidades, la sociedad civil, los verificadores, las plataformas tecnológicas y los organismos internacionales. Esa gobernanza debe permitir intercambio oportuno de información, protocolos comunes y respuestas coordinadas.

La cuarta capacidad es comunicativa. Las autoridades deben informar con rapidez, claridad y credibilidad. En un entorno de desinformación, la comunicación institucional no puede ser tardía, técnica o meramente reactiva. Debe producir un discurso confiable basado en evidencia técnica, explicar decisiones de manera ágil y sencilla, advertir sobre contenidos falsos, ofrecer herramientas de verificación y fortalecer la alfabetización digital. La ciudadanía necesita saber no solo qué se resolvió, sino también por qué se decidió así, cuáles eran los valores democráticos en riesgo y los resortes tecnológicos detrás de ellos.

La quinta capacidad es de acceso y pedagogía pública. La tecnología puede acercar la justicia electoral, pero también ampliar brechas. Se requieren materiales accesibles, lenguaje ciudadano, traducciones, herramientas de consulta, capacitación a partidos y candidaturas, y programas de alfabetización digital desde edades tempranas. La justicia electoral cercana, en clave digital, supone comprender cómo se informa la ciudadanía y cómo se forman sus preferencias en entornos algorítmicos.

La siguiente habilidad reside en la supervisión humana. Las instituciones pueden usar IA para sistematizar información, consultar precedentes o identificar patrones, pero las decisiones públicas deben permanecer bajo responsabilidad humana. La transparencia, la trazabilidad y la explicabilidad son condiciones para evitar sesgos, discriminación y opacidad. El carácter auxiliar de la IA debe convertirse en un principio transversal.

Por último, se requiere una capacidad de evaluación permanente. Las tecnologías cambian más rápido que las normas. Por eso, el Estado debe contar con mecanismos

de monitoreo, evaluación de impacto, actualización regulatoria y revisión de prácticas. Una regulación cerrada o estática puede quedar obsoleta muy pronto en términos tecnológicos; una regulación flexible, pero sin controles puede ser ineficaz. El resto es construir una gobernanza anticipatoria capaz de aprender durante cada proceso electoral y, en ese sentido, redefinir en cada ciclo su correspondiente mapa de riesgos.

Conclusiones

La justicia electoral mexicana se encuentra inmersa en una profunda transformación tecnológica. Durante décadas, sus principales tareas fueron construir certeza, legalidad, control de resultados, protección de derechos político-electorales y equidad en medios tradicionales. Hoy debe continuar asumiendo esa responsabilidad, pero en una era algorítmica; debe comprender cómo las plataformas ordenan el debate, cómo la IA produce contenido, cómo se segmentan audiencias a partir de los datos y cómo la desinformación puede modificar percepciones antes de que el derecho llegue a reaccionar.

Este nuevo escenario exige evitar respuestas simplistas. La IA no es enemiga de la democracia; puede mejorar el acceso a la justicia, traducir información, sistematizar jurisprudencia, facilitar búsquedas, acercar servicios y hacer más comprensible el derecho. Pero tampoco es neutral; puede fabricar evidencia, suplantar identidades, automatizar propaganda, explotar datos sensibles, amplificar sesgos y erosionar la realidad compartida.

El principio rector debe ser la prevención de los riesgos para la democracia, no la prohibición abstracta del uso de herramientas. La regulación debe concentrarse en la suplantación, el engaño material, la opacidad, la manipulación de datos, la desinformación deliberada y las afectaciones a la equidad. Al mismo tiempo, debe proteger la libertad de expresión, la crítica política, la sátira, el periodismo, la innovación y la participación ciudadana espontánea.

La jurisprudencia electoral debe evolucionar hacia criterios que integren el contexto tecnológico. No basta preguntar si un mensaje existió. Debe preguntarse cómo se produjo, quién lo pagó, qué datos usó, a quién fue dirigido, qué sistema lo amplificó, si fue etiquetado, si existe trazabilidad, si simuló una identidad, si afectó derechos o si tuvo capacidad real de incidir en la contienda. Esta mirada requiere peritajes, trabajo interdisciplinario y motivación reforzada.

Las plataformas digitales deben asumir deberes de cooperación y transparencia. No se trata de trasladarles la función estatal ni de convertirlas en censoras privadas, sino de reconocer que administran infraestructuras centrales para la deliberación democrática. Bibliotecas de anuncios, repositorios de propaganda, etiquetado de contenido sintético, preservación de evidencia, canales de respuesta rápida, adecuación de sus políticas internas a los estándares internacionales sobre el uso de IA y auditorías independientes son medidas compatibles con la libertad de expresión si se diseñan con proporcionalidad.

El modelo mexicano también debe atender la temporalidad electoral. Las soluciones ordinarias pueden ser insuficientes cuando el daño ocurre durante la veda, la jornada electoral o días previos a la elección. En esos momentos, la velocidad institucional es parte de la tutela efectiva. Deben existir medidas cautelares, rectificaciones, etiquetas, retiros proporcionados y revisión judicial posterior, con estándares claros para evitar censura.

La microsegmentación obliga a repensar la equidad. En el siglo XX, la preocupación era que el dinero comprara acceso desigual a radio y televisión; en el siglo XXI, hay que sumar el problema de que datos, algoritmos y opacidad permitan dirigir discursos distintos a cada persona votante sin deliberación común. La equidad debe comprender también el poder informacional y la capacidad de manipulación personalizada.

La desinformación exige diferenciar el error, la opinión, la exageración, la sátira, la crítica y la falsedad deliberada. La doctrina de la real malicia puede servir como filtro de responsabilidad ulterior, pero no como instrumento de sanción estructural. La democracia debe proteger el debate político intenso, incluso incómodo; pero no está obligada a tolerar campañas coordinadas de falsificación material diseñadas para engañar al electorado.

La justicia electoral cercana, en este contexto, no es solo una justicia territorialmente presente. Es una justicia con solvencia técnica, claridad en su comunicación, accesible por medio de herramientas digitales y democráticamente responsable. Debe acercarse a la ciudadanía en el espacio en el que se informa, discute y decide: en plataformas digitales, grupos de mensajería, buscadores, videos cortos, redes sociales y, especialmente, sistemas mediados por algoritmos.

La conclusión general puede formularse en una idea: la democracia no debe quedar subordinada a la arquitectura privada de las plataformas ni a la velocidad de la IA. El derecho electoral debe construir reglas que preserven una realidad pública verificable, una competencia equitativa y un voto libre. El desafío no es detener la tecnología, sino impedir que la simulación, la opacidad y la manipulación se conviertan en las nuevas reglas de la política.



Diálogos regionales



Tijuana, Baja California
Universidad Autónoma de Baja California



Contexto regional

La mesa sobre inteligencia artificial (IA), plataformas digitales y elecciones celebrada en la Universidad Autónoma de Baja California abrió —como parte del proyecto *Justicia electoral cercana diálogos sobre nuestra democracia*— una discusión central para el presente y el futuro de la integridad electoral. A diferencia de otros temas, en los que el debate se articula a partir de categorías jurídicas más consolidadas, aquí la conversación partió de un campo en transformación acelerada: la expansión de herramientas algorítmicas, redes sociales, plataformas privadas, datos masivos, microsegmentación, propaganda digital, contenidos sintéticos y nuevas formas de manipulación política.

Como ciudad fronteriza, tecnológica, dinámica y con una vida pública atravesada por intensos flujos migratorios, comunicación digital y participación ciudadana, Tijuana ofreció un entorno propicio para discutir cómo la democracia se desplaza hacia espacios digitales que no fueron diseñados en su origen para la deliberación pública, pero que hoy inciden de manera directa en la formación de preferencias políticas. En este contexto, la mesa permitió analizar tanto las oportunidades como los riesgos de la IA en el ámbito electoral.

La conversación reunió miradas jurisdiccionales, técnicas y académicas. Desde la visión jurisdiccional, se expuso cómo el Tribunal Electoral del Poder Judicial de la Federación (TEPJF) ha comenzado a incorporar herramientas tecnológicas en su labor interna, pero también cómo enfrenta controversias derivadas del uso de IA por actores políticos en campañas y procesos electorales. Desde la sociedad civil y la experiencia tecnológica, se analizó el impacto de la microsegmentación, la huella digital, el uso masivo de datos, la publicidad personalizada y la necesidad de que autoridades, empresas tecnológicas y ciudadanía hablen un lenguaje común.

Desde la academia, se planteó la urgencia de incorporar nuevos principios —como ciberseguridad y ética digital— al debate electoral, así como de pensar modelos de regulación, etiquetado, monitoreo y sanción frente a *deepfakes*, campañas de desinformación y manipulación algorítmica.

Un rasgo relevante de la sede fue que la IA no fue presentada solo como amenaza en sí. Por el contrario, se le reconoció como herramienta de apoyo tanto para la función jurisdiccional como para la participación ciudadana, la sistematización de información, la mejora de servicios públicos y la eventual inclusión de grupos que enfrentan barreras lingüísticas o tecnológicas. En el ámbito interno del TEPJF se mencionaron ejemplos concretos: el juicio en línea, la herramienta Alfonsina —alimentada con precedentes, sentencias y jurisprudencia— y el uso de la aplicación Copilot para sistematizar información y apoyar en tareas de análisis jurídico. Sin embargo, también se subrayó que estas herramientas dependen de la calidad de los datos, de la protección de la información y de la supervisión humana.

También destacó el reconocimiento de que los actores políticos ya utilizan tecnologías digitales en campañas y contiendas. La IA puede generar imágenes, voces, videos, textos, mensajes personalizados y contenidos en apariencia reales. Las plataformas pueden amplificar mensajes a velocidades inéditas. La microsegmentación permite hablarle a cada persona de forma distinta según su edad, hábitos de consumo, ubicación, intereses, comportamiento digital o vulnerabilidad emocional. Esto modifica las condiciones de la competencia electoral: la equidad ya no depende solo del dinero, los tiempos oficiales o el acceso a medios tradicionales, sino también del acceso a datos, algoritmos y de la capacidad de segmentación.

La sede Tijuana permitió plantear una premisa central: la democracia mexicana ya opera en una era algorítmica, pero su marco jurídico, institucional y educativo aún conserva una lógica en buena medida analógica. El desafío es construir una justicia electoral capaz de proteger la libertad de expresión y el debate público, sin permitir que la desinformación, la opacidad algorítmica o la manipulación personalizada deterioren la autenticidad del voto.



Problemas o tensiones jurídicas

La mesa reconoció que en México aún no existe una regulación integral sobre IA en materia electoral. Aunque hay iniciativas legislativas y criterios en construcción, las autoridades administrativas y jurisdiccionales electorales han tenido que resolver caso por caso, utilizando categorías tradicionales como libertad de expresión, calumnia,

propaganda electoral, interés superior de la niñez, violencia política contra las mujeres en razón de género, veda electoral o deber de imparcialidad. La dificultad reside en que esas categorías fueron diseñadas para un entorno comunicativo distinto.

Otra tensión fue la relación entre IA y la función jurisdiccional. En el ámbito interno, la IA puede servir para sistematizar precedentes, facilitar búsquedas, organizar expedientes, mejorar el acceso ciudadano y hacer más eficiente el trabajo jurídico. Sin embargo, también plantea preguntas delicadas: ¿qué tipo de información alimenta los sistemas?, ¿cómo se protege la confidencialidad?, ¿hasta dónde puede automatizarse una tarea jurisdiccional?, ¿qué debe seguir siendo una decisión humana?, y ¿cómo evitar que una herramienta reproduzca errores, sesgos o respuestas incorrectas? La discusión dejó claro que la IA debe entenderse como una herramienta de apoyo, no como sustituto del criterio jurídico.

También se identificó como problema la detección de contenidos generados con IA. Se expusieron casos en los que partidos o candidaturas han utilizado imágenes de niñas, niños o adolescentes en apariencia creadas mediante IA, lo que generó dudas sobre si era aplicable la protección del interés superior de la niñez cuando no se acreditaba la existencia de una persona menor de edad real. Este tipo de casos muestra que las categorías tradicionales de consentimiento, imagen, identidad y protección de personas menores de edad deben adaptarse a los contenidos sintéticos. La pregunta ya no es solo si una persona aparece en propaganda, sino si una imagen artificial puede producir efectos políticos, emocionales o engañosos equivalentes.

A ello se sumó la tensión vinculada con la violencia política y la viralización. Las redes sociales pueden convertir un comentario, una imagen o un video en un fenómeno masivo antes de que la autoridad pueda reaccionar. En casos de violencia política contra las mujeres, calumnia o desinformación, la velocidad de circulación del contenido supera los tiempos ordinarios de investigación, adopción de medidas cautelares y sanción. Esto genera un problema de eficacia: cuando la decisión llega, el daño comunicativo ya pudo haberse producido.

Otro aspecto relevante fue la microsegmentación política. Como se sabe, a partir de la huella digital, las plataformas pueden clasificar audiencias y dirigir mensajes distintos a grupos específicos. Esto modifica el carácter público del debate electoral. En la propaganda tradicional, un mensaje puede ser discutido, contrastado, criticado o fiscalizado por todos. En la propaganda microsegmentada, en cambio, un mensaje puede ser visible solo para ciertas personas, sin que el resto de la ciudadanía, los medios o las autoridades conozcan su contenido. Esto dificulta la rendición de cuentas y

permite la difusión de mensajes contradictorios, campañas de miedo, desmovilización selectiva o manipulación emocional.

Otra conversación giró en torno a la relación entre plataformas privadas y autoridades electorales. Las redes sociales no fueron creadas como órganos electorales, sino como empresas tecnológicas y publicitarias con fines de lucro. Sin embargo, hoy son espacios centrales de comunicación política y, en este sentido, forman parte de la esfera pública. El diálogo destacó la necesidad de colaboración con plataformas como Meta, en especial para identificar noticias falsas, perfiles inauténticos, *bots* o contenidos problemáticos. Pero también se advirtió que la colaboración no basta, debe discutirse la responsabilidad compartida, la representación jurídica de plataformas en México, la trazabilidad de anuncios, la respuesta a requerimientos de información y el cumplimiento de órdenes electorales.

Se observó, además, la dificultad probatoria derivada del anonimato. Esto es, muchos contenidos desinformativos o manipuladores provienen de perfiles anónimos, cuentas falsas, *bots* o redes de amplificación difíciles de rastrear. Esto complica la identificación de sujetos responsables y limita la eficacia de las sanciones. El diálogo señaló que, en algunos casos, el TEPJF ha recurrido a catálogos de sujetos sancionados o registros indeterminados cuando no es posible identificar por completo a la persona detrás del perfil. Sin embargo, ese tipo de respuesta todavía es insuficiente frente a campañas coordinadas o al financiamiento opaco.

Otro punto de tensión fue la relación entre la regulación y la libertad de expresión. La discusión subrayó que no debe sancionarse la IA en sí misma, sino los contenidos o usos que vulneren principios electorales. Una regulación excesiva podría abrir la puerta a censura, control del discurso político o inhibición indebida de la crítica. Pero una ausencia total de reglas puede permitir manipulación, *deepfakes*, calumnias, propaganda encubierta o interferencia indebida. La clave está en construir una regulación proporcional que distinga entre sátira, opinión, crítica, error, contenido sintético legítimo y desinformación intencionada con capacidad de afectar la elección.

Al cierre, se identificó un problema educativo y democrático: la manipulación digital no se combate solo con sanciones, sino también mediante la formación de una ciudadanía crítica. En contextos de bajo nivel educativo, brechas digitales o desinformación persistente, las personas pueden quedar expuestas a contenidos falsos o mensajes dirigidos a influir en el plano emocional. Por ello, la alfabetización digital, la educación cívica y la capacidad de contrastar fuentes son condiciones de la integridad electoral.

Aportes conceptuales

Un aporte conceptual relevante de Tijuana fue entender la democracia contemporánea como democracia algorítmica. La deliberación pública ya no ocurre solo en plazas, medios impresos, radio, televisión o mítines. Ocurre en plataformas mediadas por algoritmos que jerarquizan, recomiendan, amplifican u ocultan información. Esto obliga a repensar la justicia electoral, pues ya no basta con vigilar *spots*, bardas o tiempos oficiales; también debe observarse cómo circula, se segmenta y se potencia la información política.

También fue relevante distinguir entre el uso interno y externo de la IA. En el ámbito interno, la IA puede mejorar acceso a la justicia, organización de información, análisis de precedentes y eficiencia institucional. En el ámbito externo, puede ser utilizada por actores políticos para propaganda, segmentación, manipulación, desinformación o generación de contenidos sintéticos. Esta distinción evita visiones simplistas: la IA no es buena o mala por sí misma; su impacto depende del uso, finalidad, contexto, transparencia y controles.

Otra idea que destacó fue que la equidad electoral también debe pensarse en términos de datos. La equidad, tradicionalmente, se ha regulado en ámbitos como financiamiento, tiempos de radio y televisión, fiscalización y propaganda. Pero en el entorno digital, quien posee más datos y mejores herramientas de segmentación puede adquirir ventajas estructurales en una competencia electoral. Así, esta puede volverse desigual no solo por dinero visible, sino por el acceso invisible a bases de datos, modelos predictivos, pauta digital y capacidad de personalizar mensajes.

Se planteó que los modelos comparados tienden a regular la propaganda generada con IA a partir de dos principios: transparencia y etiquetado. Esto implica saber cuándo un contenido fue producido o alterado con IA, quién lo generó, quién lo pagó, a quién se dirigió y con qué criterios de segmentación circuló. El etiquetado permite proteger el debate sin prohibir toda innovación tecnológica.

En esta línea, se subrayó la relevancia de incorporar ciberseguridad y ética digital a los principios electorales. Las elecciones mexicanas se han construido alrededor de certeza, legalidad, imparcialidad, objetividad y equidad. La mesa sugirió que, en la era digital, estos principios deben complementarse con nuevas exigencias: trazabilidad de datos, seguridad tecnológica, integridad informativa, protección de datos personales, transparencia algorítmica y responsabilidad en el uso de IA.

Una noción en particular interesante que surgió durante el diálogo fue la de justicia electoral algorítmica. Esta noción no se planteó en el sentido de sustituir a las personas juzgadoras por máquinas, sino en el sentido de reconocer que la justicia electoral ya resuelve conflictos originados en redes, plataformas, algoritmos, contenidos sintéticos y datos masivos. La justicia electoral algorítmica exige nuevos criterios probatorios, nuevas capacidades técnicas y nuevas formas de ponderar libertad de expresión, la autenticidad del voto y la integridad del debate público.

Asimismo, la regulación no puede construirse solo desde el derecho electoral ni solo desde la tecnología. Requiere diálogo entre autoridades electorales, tribunales, plataformas, academia, especialistas en datos, organizaciones civiles, partidos, centros de investigación y ciudadanía. La discusión subrayó que el derecho, la tecnología y la democracia deben articularse en un mismo espacio de diálogo para asegurar una colaboración multinivel.

Por último, se mencionó el vínculo indispensable entre innovación y control democrático. Es decir, la IA puede apoyar traducción, accesibilidad, análisis de datos, simplificación de trámites, monitoreo de compromisos, detección de patrones y mejora institucional. Pero esas oportunidades solo serán democráticas si se acompañan de ética, regulación, supervisión humana, transparencia y rendición de cuentas.



Conclusiones, propuestas y líneas de acción

La principal conclusión de la sede Tijuana fue que la IA y las plataformas digitales ya forman parte estructural de los procesos electorales. No son un fenómeno futuro ni marginal. Por ello, la justicia electoral debe abandonar una lógica solo reactiva y construir capacidades normativas, técnicas, educativas e institucionales para enfrentar la manipulación digital sin inhibir la libertad de expresión ni el uso legítimo de herramientas tecnológicas.

Una ruta de trabajo consiste en construir un marco normativo especial sobre IA y elecciones. Este marco debe regular contenidos sintéticos, *deepfakes*, propaganda digital, microsegmentación, *bots*, financiamiento de pauta, *dark ads*, uso de datos personales, trazabilidad de anuncios y obligaciones de transparencia. La regulación debe ser proporcional: no debe prohibir la tecnología, sino los usos que engañen, manipulen o vulneren derechos.

También conviene establecer reglas o criterios judiciales respecto de la transparencia y el etiquetado. Todo contenido político generado o alterado en grado sustancial con IA debería identificarse con claridad. También debería informarse quién lo produce,

quién lo paga, cuál es su público objetivo y si fue difundido mediante segmentación. El etiquetado puede ser una herramienta útil para proteger el derecho a la información sin censurar contenidos.

A ello se suma un reto central: regular la microsegmentación política. Deben definirse límites a la utilización de datos personales, perfiles psicológicos, vulnerabilidades emocionales, información sensible o mensajes contradictorios según la audiencia. La propaganda electoral no debe convertirse en comunicación invisible e imposible de fiscalizar. La ciudadanía tiene derecho a saber qué mensajes circulan en una campaña, incluso cuando esos mensajes no fueron dirigidos a ella.

Otra propuesta apunta a crear un sistema de monitoreo electoral digital. El diálogo planteó la posibilidad de un modelo híbrido, multinivel y coordinado, con participación de autoridades electorales, universidades, centros de investigación y especialistas técnicos. Este sistema podría monitorear contenidos públicos, detectar patrones de desinformación, identificar campañas coordinadas, generar alertas, preservar evidencia y apoyar a las autoridades sin sustituir sus funciones.

También conviene fortalecer la colaboración con las plataformas, pero a partir de reglas de responsabilidad. La relación con empresas tecnológicas no debe depender solo de la buena voluntad. Deben existir canales institucionales claros, plazos de respuesta, representación jurídica, protocolos de preservación de evidencia, mecanismos para atender órdenes electorales y criterios de responsabilidad cuando una plataforma facilite o tolere prácticas que afecten la integridad electoral.

Asimismo, es necesario desarrollar capacidades técnicas en las autoridades electorales y jurisdiccionales. Juzgar controversias digitales exige comprender cómo funcionan los algoritmos, la pauta, los *bots*, los metadatos, la generación de contenido sintético, la viralización y la segmentación. Se requiere capacitación continua, glosarios comunes, peritajes especializados, laboratorios de análisis digital y formación conjunta entre juristas y especialistas en tecnología.

Otra ruta de trabajo apunta a diseñar criterios probatorios para IA y desinformación. Las autoridades deben saber cómo acreditar que un contenido fue generado o manipulado con IA, cómo vincularlo con una candidatura o partido, cómo medir su alcance, cómo valorar su capacidad real de influir en la elección y cómo distinguir contenido falso, sátira, opinión, error o manipulación dolosa. Sin reglas probatorias claras, la sanción será difícil o arbitraria.

A ello se agrega la necesidad de proteger el interés superior de la niñez y la dignidad de las personas frente a contenidos sintéticos. Deben desarrollarse lineamientos

para imágenes generadas con IA que representen niñas, niños, adolescentes, mujeres, personas candidatas o grupos vulnerables. Aunque una imagen no corresponda a una persona real, puede producir efectos políticos, emocionales o discriminatorios que deben ser analizados.

La agenda también incluye fortalecer la educación cívica digital con miras a que la ciudadanía aprenda a identificar *deepfakes*, *bots*, publicidad segmentada, cadenas falsas, noticias fabricadas y manipulación emocional. Esta formación debe iniciar desde la educación básica y continuar mediante campañas públicas, materiales accesibles, aplicaciones, alianzas con universidades y ejercicios de verificación ciudadana.

Como cierre operativo, se propone establecer mayores deberes para personas servidoras públicas y candidaturas. Quienes aspiran a cargos o ejercen funciones públicas utilizan recursos, espacios y confianza pública. Por ello, deben tener estándares reforzados frente al uso de IA, desinformación, propaganda encubierta o manipulación digital. La responsabilidad debe ser mayor cuando la conducta proviene de actores con poder institucional.

La sede Tijuana, en términos generales, ofreció una conclusión clave: la IA no amenaza por sí misma a la democracia; lo que la amenaza es su uso opaco, irresponsable, desigual o manipulador. La justicia electoral cercana debe comprender la tecnología, no temerle; regularla, no prohibirla de forma absoluta; aprovecharla, sin delegar en ella la decisión humana, y ponerla al servicio de una ciudadanía más informada, libre y crítica. La principal contribución de esta sede fue mostrar que la integridad electoral del siglo XXI dependerá de la capacidad institucional para entender datos, algoritmos, plataformas y contenidos sintéticos, sin perder de vista el núcleo democrático: la libertad de expresión, la equidad en la contienda, el derecho a la información, la autenticidad del voto y la confianza pública.

Arteaga, Coahuila
Academia Interamericana de Derechos Humanos



Contexto regional

Al desarrollarse en una institución especializada en derechos humanos, la discusión en la sede Arteaga no se limitó a la dimensión tecnológica del problema, sino que incorporó una preocupación constitucional más amplia: ¿cómo armonizar innovación, libertad de expresión, protección de datos personales, derecho a la información, libre desarrollo de la personalidad, equidad en la contienda, imparcialidad de los procesos electorales y tutela judicial efectiva? La IA fue abordada no solo como herramienta técnica, sino como fenómeno que puede modificar las condiciones de ejercicio de los derechos políticos.

Arteaga permitió, así, avanzar más allá de la pregunta general sobre si debe regularse la IA. El debate se concentró en cómo regular sin inhibir la innovación, cómo sancionar sus usos dañinos sin censurar el discurso público, cómo utilizarla para mejorar la justicia electoral sin sustituir la deliberación humana y cómo construir capacidades institucionales para que las autoridades puedan comprender, probar y resolver conflictos digitales con rapidez y rigor técnico.

Si Tijuana abrió la discusión sobre la democracia algorítmica, Arteaga profundizó en los problemas de evidencia, trazabilidad, responsabilidad, límites jurídicos y diseño institucional necesarios para que la justicia electoral pueda operar en un entorno digital cada vez más complejo.



Problemas o tensiones jurídicas

Un problema central fue la ausencia de una regulación precisa sobre IA en México. La mesa reconoció que existen principios

constitucionales y normas generales aplicables —la libertad de expresión, el derecho a la información, la protección de datos, la equidad electoral, el interés superior de la niñez, la calumnia, la violencia política y la propaganda electoral—, pero no un marco específico que atienda de forma integral los usos de IA en procesos electorales. Esto ha obligado al TEPJF a resolver caso por caso, construyendo precedentes frente a situaciones que el legislador aún no ha desarrollado.

Se mencionó, a su vez, la utilización de imágenes, videos o audios generados con IA en propaganda electoral. La discusión partió de casos en los que se usaron imágenes de niñas, niños o adolescentes creadas mediante IA. Este supuesto genera una tensión novedosa: si la imagen no corresponde a una persona menor de edad real, puede no existir una afectación directa al derecho de imagen de una niña o niño concreto; pero el contenido sí puede producir efectos comunicativos, emocionales o propagandísticos. Por ello, se planteó la necesidad de etiquetar contenidos generados con IA y de actualizar lineamientos para que la ciudadanía sepa cuándo está frente a un contenido sintético.

A ello hay que sumar la tensión vinculada con la suplantación de identidad o la alteración de imágenes y audios. La IA permite crear videos, audios o imágenes en los que una persona parece decir o hacer algo que nunca dijo o hizo. En campañas electorales, esto puede afectar la reputación, el honor, la libertad de expresión, el derecho a la información y la equidad en la contienda. La mesa fue clara: no puede permitirse la utilización de IA para suplantar la voluntad, la imagen, la voz o la personalidad de una candidatura, una persona servidora pública o un actor político sin consentimiento.

En esta línea, un punto de encuentro fue que no toda información incorrecta debe ser sancionada, pues el debate público admite la crítica, el error, la sátira, la opinión y la exageración. Sin embargo, la desinformación intencionada implica algo distinto: contenido que no coincide con la realidad, difundido con conocimiento o intención de engañar, capaz de manipular el voto o distorsionar la voluntad política. La mesa vinculó este tema con la doctrina de la real malicia, la falsedad verificable y la capacidad del contenido para afectar la decisión ciudadana.

Como era de esperarse, surgió nuevamente el complejo tema de la creación y distribución de contenido bajo una lógica de microsegmentación. Por medio de *big data* y modelos algorítmicos, los actores políticos pueden dirigir mensajes diferenciados a grupos específicos de personas según sus hábitos de consumo, religión, ubicación, preferencias, edad, condición socioeconómica, emociones o comportamiento digital. Esto puede afectar la equidad en el acceso a la información

y la transparencia del debate público. Una campaña puede decir una cosa a un segmento de la población y lo contrario a otro, sin que exista una huella visible para el conjunto de la ciudadanía. La deliberación democrática se fragmenta y se vuelve difícil de fiscalizar.

Un reto no menor se ubica en el ámbito probatorio. En efecto, para resolver un caso relacionado con IA, la autoridad debe determinar si un contenido fue generado mediante IA, quién lo produjo, quién lo difundió, quién lo financió, qué alcance tuvo y si pudo afectar la contienda. Pero los procedimientos electorales son breves y exigen justicia pronta. La mesa identificó una tensión entre el tiempo y costo necesarios para un peritaje técnico y la urgencia de dictar medidas cautelares o resolver antes de que el daño electoral se consume. En campañas, la demora puede volver inútil la decisión.

En la operación jurídica siempre es un desafío identificar a los responsables de cierta conducta penada o prohibida; sin embargo, esto se complejiza aún más en el mundo digital. Los contenidos generados con IA circulan en redes sociales, perfiles anónimos, cuentas falsas, *bots* o sistemas de mensajería privada. Esto dificulta atribuir responsabilidad a una candidatura, partido, persona servidora pública o tercero. La mesa reconoció que incluso si se diseñan sanciones económicas o medidas correctivas, su eficacia depende de identificar al responsable y probar el vínculo entre la conducta y el actor político beneficiado.

Ante estas problemáticas, habría que preguntarse si las autoridades administrativas y judiciales cuentan con las capacidades institucionales adecuadas para hacer frente a aquellas. Es decir, para juzgar controversias digitales, las autoridades electorales requieren conocimientos sobre algoritmos, metadatos, autenticidad de imágenes, modelos generativos, perplejidad, variación natural del lenguaje, trazabilidad, estándares técnicos, evidencia digital y normas internacionales. Sin esas capacidades, el derecho puede llegar tarde o resolver con categorías insuficientes.

Por último, se identificó una tensión entre regulación y actualización tecnológica. Una ley demasiado detallada puede quedar obsoleta con rapidez, debido a la velocidad con que evolucionan los modelos de IA. Pero la ausencia de regulación deja a la ciudadanía y a las autoridades sin parámetros claros. La sede Arteaga mostró que el reto no es elegir entre ley rígida o vacío normativo, sino construir un modelo flexible, basado en principios, estándares técnicos, lineamientos actualizables y coordinación interinstitucional.



Aportes conceptuales

Un aporte conceptual de especial importancia de Arteaga fue entender la IA como medio comisivo y no necesariamente como conducta ilícita en sí misma. La IA no debe ser prohibida por su sola existencia. Lo relevante desde el punto de vista jurídico es el uso que se le da: si sirve para informar, sistematizar, traducir o facilitar el acceso, puede fortalecer la democracia al incentivar la participación ciudadana; si se utiliza para suplantar identidades, fabricar desinformación, manipular audiencias o vulnerar derechos, debe ser regulada y sancionada.

Una distinción clave es la que existe entre contenido sintético legítimo y contenido sintético engañoso. No todo el contenido generado con IA es problemático. Puede utilizarse en educación cívica, accesibilidad, traducción, análisis de información o comunicación institucional. El problema surge cuando el contenido pretende pasar por real, oculta su origen artificial, distorsiona hechos verificables o manipula la voluntad ciudadana. De ahí la importancia del etiquetado.

En el entorno digital, la transparencia no debe limitarse a saber quién compró un espectacular o un *spot*. Debe incluir quién generó un contenido, si fue creado o alterado con IA, qué datos se utilizaron para dirigirlo, a qué segmento se envió, cuánto se pagó por su difusión y qué criterios de segmentación fueron empleados. La transparencia algorítmica se vuelve una condición de la equidad electoral.

Otra aportación fue la idea de trazabilidad del contenido en el entendido de que para proteger la integridad electoral no basta con retirar publicaciones. Es necesario, además, preservar evidencia, conocer origen, ruta de circulación, modificaciones, metadatos, alcance y vínculos de financiamiento. La trazabilidad permite pasar de una intuición sobre manipulación a una prueba desde el punto de vista jurídico utilizable.

Se observó, además, la identificación de tres límites materiales al uso político-electoral de IA: no suplantar la personalidad o voluntad de una persona, no generar desinformación mediante *fake news* y no utilizar microconversaciones o segmentación masiva para manipular de modo indebido al electorado. Estos tres límites ofrecen una base inicial para construir criterios regulatorios y jurisdiccionales.

En cuanto a los modelos regulatorios, la mesa no propuso que las plataformas actúen sin control público ni que el Estado decida de forma unilateral todo contenido. Se planteó, más bien, un modelo intermedio: mecanismos de autorregulación por

parte de plataformas, pero con seguimiento, evaluación y supervisión de autoridades electorales. Esto permitiría respuestas rápidas sin renunciar a las garantías.

Por último, se apuntó el impacto de la desinformación en la legitimidad de la voluntad política. En la discusión se señaló que el bien jurídico protegido no es solo la verdad abstracta, sino la posibilidad de que la ciudadanía forme su voluntad política de forma libre e informada. La manipulación digital afecta la democracia porque deteriora las condiciones de autonomía del voto.



Conclusiones, propuestas y líneas de acción

Una línea de acción apunta a desarrollar un marco regulatorio flexible sobre IA y elecciones. Este marco debe establecer principios generales, reglas de transparencia, obligaciones de etiquetado, protección de datos, límites a la microsegmentación, sanciones por suplantación y criterios para combatir la desinformación intencionada. Debe evitar una regulación en exceso rígida que quede obsoleta, pero también debe superar el vacío actual.

A ello se suma la necesidad de exigir el etiquetado de contenidos generados o alterados con IA. La ciudadanía tiene derecho a saber si una imagen, un video, un audio o un texto político es sintético. El etiquetado no impide el uso de IA, pero permite evaluar el contenido con información suficiente. Esta medida resulta de especial relevancia en la propaganda electoral y en contenidos relacionados con candidaturas, niñas, niños, mujeres, grupos vulnerables o hechos verificables.

Es indispensable impulsar protocolos respecto a los *deepfakes*; estos contenidos que suplantan voz, rostro, imagen o la identidad de una persona deben recibir tratamiento prioritario. Las autoridades deben contar con mecanismos rápidos de verificación, preservación de evidencia, medidas cautelares, retiro proporcional de contenidos y sanciones cuando exista dolo, afectación a derechos o riesgo para la equidad de la contienda.

Una propuesta adicional consiste en crear capacidades periciales especializadas. La justicia electoral necesita peritos, laboratorios, herramientas y estándares técnicos para analizar contenido digital. La determinación de si un contenido fue generado mediante IA no puede depender solo de la percepción visual. Deben desarrollarse metodologías para revisar metadatos, patrones lingüísticos, origen de archivos, trazabilidad, manipulación audiovisual y sistemas de generación utilizados. A ello se suma la necesidad

de desarrollar lineamientos sobre propaganda con niñas, niños y adolescentes. Los contenidos sintéticos que representan a personas menores de edad plantean problemas nuevos. Aunque no exista una niña o un niño real, la imagen puede ser utilizada para generar emociones, manipular percepciones o simular apoyo social. Se requiere una regulación que atienda tanto la protección de personas reales como los efectos comunicativos de las imágenes artificiales.

Otro frente clave es la colaboración con las plataformas digitales bajo un esquema de responsabilidad compartida. Las plataformas deben contar con canales de comunicación con las autoridades electorales, mecanismos de respuesta urgente, protocolos de preservación de evidencia, transparencia en publicidad política y procedimientos para retirar contenidos ilícitos. Esta colaboración debe estar sujeta a reglas claras y revisión pública, no a la discrecionalidad privada, pues la finalidad es que sus políticas internas sean garantistas del orden constitucional.

Es importante reflexionar acerca de qué sanciones económicas y electorales establecer y cómo hacerlas proporcionales. El diálogo planteó la posibilidad de sanciones económicas frente a usos de IA que suplanten identidades, generen desinformación o manipulen al electorado. Además, en casos graves, podrían considerarse efectos electorales cuando se acredite impacto real en la contienda, dolo, financiamiento, coordinación y capacidad de alterar la voluntad ciudadana.

Una línea de acción no menor es fortalecer la educación digital y su impacto en el mundo electoral; la ciudadanía debe aprender a identificar contenidos generados con IA, *deepfakes*, noticias falsas, propaganda segmentada y manipulación emocional. Esta educación debe dirigirse también a partidos, candidaturas, autoridades, medios y personas servidoras públicas. Sin alfabetización digital, la regulación será insuficiente.

La sede Arteaga dejó una conclusión medular: la IA no debe ser vista como enemiga de la democracia, pero tampoco como una herramienta neutral. Su impacto depende de quién la usa, con qué datos, con qué finalidad, con qué controles y con qué efectos. La justicia electoral cercana debe ser capaz de comprender también el lenguaje técnico de la era digital, para proteger mejor la voluntad ciudadana. En este sentido, la justicia electoral del futuro necesitará no solo buenos argumentos jurídicos, sino también capacidades tecnológicas para detectar, probar y frenar manipulaciones digitales. En la era de la IA, proteger la democracia exige proteger la información, la identidad, la autonomía del voto y la confianza pública.

Morelia, Michoacán
Universidad Michoacana de San Nicolás de Hidalgo



Contexto regional

La sede michoacana ofreció un entorno universitario propicio para discutir no solo los riesgos jurídicos de la IA, sino también sus implicaciones culturales, comunicativas y educativas. El seminario partió de una premisa compartida: las nuevas tecnologías ya no son un fenómeno periférico de los procesos electorales. La IA, las redes sociales, los algoritmos de recomendación, la microsegmentación, la publicidad digital, los *bots*, los *deepfakes* y la extracción masiva de datos forman parte del ecosistema ordinario de la comunicación política.

En este nuevo entorno, la justicia electoral enfrenta un reto doble. Por un lado, debe proteger la libertad de expresión y permitir que la tecnología contribuya a informar mejor a la ciudadanía. Por otro, debe prevenir que esas mismas herramientas sean utilizadas para manipular, desinformar, suplantar identidades o distorsionar la voluntad del electorado.

Morelia aportó así una mirada de especial valor pedagógico. La mesa no se quedó en la pregunta sobre la sanción del uso de IA en campañas. Su preocupación fue más amplia: cómo construir una ciudadanía capaz de distinguir la información auténtica del contenido manipulado; cómo regular las plataformas sin censurar de modo indebido; cómo atribuir responsabilidad en entornos digitales complejos; cómo evitar que la microsegmentación convierta a cada votante en receptor de una realidad política distinta, y cómo lograr que la IA sea parte de la solución, no solo del problema.

La sede Morelia permitió comprender que la discusión sobre IA, plataformas y elecciones no es solo jurídica ni solo tecnológica. Es, ante todo, una discusión democrática. Lo que está en juego es la calidad de la deliberación pública, la autonomía del voto, la

confianza en la información, la responsabilidad de los actores políticos y la capacidad institucional para responder a una ola tecnológica sin precedentes.



Problemas o tensiones jurídicas

Un problema central fue la distancia entre la velocidad tecnológica y la lentitud normativa. La discusión subrayó que la IA evoluciona con enorme rapidez, mientras que el derecho requiere procesos legislativos, reglamentarios y jurisdiccionales más pausados. Esta diferencia produce un desfase estructural: cuando se intenta regular una práctica, muchas veces la tecnología ya cambió o fue sustituida por otra. La consecuencia es que las autoridades electorales suelen actuar de forma reactiva, a partir de casos concretos, lineamientos administrativos o precedentes jurisdiccionales, en lugar de contar con un marco integral y preventivo.

La IA ha reducido la distancia entre lo real y lo simulado; esto complejiza la autenticidad de los contenidos de la conversación pública. Textos, imágenes, videos, audios y mensajes pueden producirse con tal nivel de sofisticación que resulta difícil distinguir si fueron creados por una persona, por una máquina o mediante una combinación de ambas. Esta dificultad afecta de manera directa la materia electoral porque la ciudadanía toma decisiones con base en información disponible. Si esa información es falsa, alterada o sintética y se presenta sin advertencia, la voluntad política puede formarse sobre una percepción distorsionada de la realidad.

En la mesa se recordó que, durante mucho tiempo, internet fue entendido como un espacio con protección reforzada por la libertad de expresión. Sin embargo, la experiencia electoral ha evidenciado que partidos, candidaturas y otros actores pueden utilizar redes sociales para difundir mensajes coordinados, propaganda encubierta, información falsa o contenidos generados mediante IA. El desafío consiste en proteger el debate robusto, la sátira, la crítica y la opinión ciudadana, sin permitir que la libertad de expresión se convierta en cobertura para la manipulación electoral.

Un tema novedoso fue el de la manipulación conductual basada en datos. La mesa distinguió entre la mercadotecnia tradicional y una forma más sofisticada de intervención sobre preferencias ciudadanas. Antes, la propaganda buscaba persuadir mediante mensajes públicos; ahora, los algoritmos pueden identificar momentos de mayor receptividad, intereses personales, redes de contacto y predisposiciones emocionales.

La pregunta que surgió fue profunda: si una persona vota después de recibir mensajes diseñados a partir de su perfil psicológico, sus hábitos de consumo digital y sus vulnerabilidades, ¿hasta qué punto su decisión fue libre, genuinamente autónoma?

El anonimato puede proteger la libertad de expresión, en especial frente a contextos de presión política o social, pero también puede facilitar desinformación, violencia digital, campañas negras, *bots* y manipulación sin rendición de cuentas. El diálogo planteó la necesidad de discutir mecanismos de verificación de identidad para ciertos tipos de contenido especialmente sensible, sin crear un Estado censor ni eliminar el derecho de la ciudadanía a expresarse con libertad. La tensión está en distinguir cuándo el anonimato protege la democracia y cuándo la daña.

Por otra parte, frente a un contenido electoral generado o amplificado con IA, no siempre es claro quién debe responder por este: la persona que creó el contenido, quien lo difundió, la candidatura beneficiada, el partido, la plataforma, el proveedor tecnológico o incluso quienes lo consumen y replican. La mesa sostuvo que la responsabilidad no puede recaer en un solo actor de forma abstracta. Debe analizarse caso por caso, según quién produjo, pagó, amplificó, coordinó o se benefició del contenido, así como el nivel de conocimiento, la intención y la capacidad de control.

Además, se identificó la falta de delimitación geográfica del fenómeno digital. Las campañas pueden operar desde cuentas ubicadas fuera del país, servidores extranjeros, plataformas sin representación local o redes de amplificación difíciles de rastrear. Esto desafía a las autoridades electorales, cuyo ámbito de actuación está delimitado al territorio mexicano. La comunicación digital cruza fronteras en segundos, mientras que la investigación, la obtención de pruebas y la cooperación institucional suelen requerir mucho más tiempo.

El diálogo señaló que la publicidad digital puede diluirse entre *influencers*, buscadores, plataformas, contenidos orgánicos y mensajes segmentados. Esta fragmentación dificulta fiscalizar cuánto se gasta, quién paga, qué se comunica, a quién se dirige y con qué criterios se segmenta. La fiscalización tradicional, pensada para espectaculares, *spots* o propaganda impresa, resulta insuficiente para rastrear los recursos y valorar el impacto de las campañas digitales. En síntesis: la actual regulación de la publicidad política digital es insuficiente.



Aportes conceptuales

Una contribución conceptual relevante de Morelia fue entender la IA como una revolución tecnológica que altera la percepción de la realidad. A diferencia de tecnologías anteriores, que eran controladas de manera directa por personas, la IA produce contenidos, respuestas, imágenes y mensajes que pueden parecer autónomos o auténticos. Esto obliga a la justicia electoral a preguntarse no solo qué se dijo, sino cómo se generó, quién lo generó, si fue alterado y si la ciudadanía pudo distinguir su naturaleza.

También fue relevante la idea del derecho como un sistema que mira hacia atrás frente a tecnologías que avanzan con rapidez. La metáfora utilizada en la mesa —el derecho como un coche rápido con retrovisor muy grande y sin parabrisas— permitió expresar una tensión estructural: el derecho regula a partir de experiencias conocidas, pero la tecnología genera situaciones nuevas antes de que existan reglas específicas. Por ello, los principios generales y los precedentes jurisdiccionales adquieren especial relevancia.

Una distinción relevante que se trazó en el diálogo fue entre el contenido generado por la ciudadanía y el creado y difundido por actores políticos sujetos a fiscalización. No todo lo que aparece en redes sociales debe ser tratado igual. Una sátira o un meme elaborado por una persona ciudadana no puede recibir el mismo tratamiento que una campaña coordinada por un partido, una candidatura o una red financiada. La justicia electoral debe cuidar que sus respuestas no inhiban la expresión ciudadana, pero sí debe actuar cuando existan indicios de coordinación, financiamiento, sistematicidad o impacto electoral relevante. ¿Cómo y en dónde trazar la línea? Ese es el reto regulatorio y jurisdiccional.

A ello se sumó la noción de integridad electoral como autenticidad de la comunicación. La integridad electoral no se agota en contar de forma correcta los votos. También exige que la ciudadanía reciba información que no esté deliberadamente distorsionada, que la propaganda sea identificable, que los mensajes no se basen en suplantaciones y que la competencia no se distorsione mediante ventajas tecnológicas opacas. En la era digital, proteger la elección implica proteger también el entorno informativo previo al voto.

Otra contribución relevante fue reconocer la microsegmentación como una forma de asimetría tecnológica. Quien posee más infraestructura, datos, conocimiento técnico y capacidad de segmentación puede incidir con mayor precisión sobre electores

específicos. Esta ventaja no siempre es visible ni fiscalizable. Por ello, la equidad en la contienda debe repensarse, pues ya no basta con medir el gasto declarado o la exposición pública general; también debe analizarse la capacidad de personalizar mensajes, segmentar audiencias de forma opaca y dirigir información a segmentos vulnerables.

A partir de varias experiencias, la mesa consideró que la pregunta central no debe ser solo qué hace la IA, sino qué debe hacer y bajo qué límites. La ética no es un complemento externo de la tecnología; debe ser su punto de partida. En materia electoral, ello implica transparencia, prevención del daño, uso responsable, trazabilidad, respeto a derechos y compromiso con la deliberación democrática.

Por último, la mesa no colocó toda la carga regulatoria en el Estado, ni toda la responsabilidad en las plataformas o las personas usuarias. Se reconoció que la integridad digital exige responsabilidades diferenciadas: de las autoridades, para regular y sancionar; de las plataformas, para actuar con transparencia; de los partidos y las candidaturas, para no manipular; de proveedores tecnológicos, para prevenir daños, y de la ciudadanía, para consumir y compartir información con criterio. En esta línea, se sumó la idea de que la regulación debe orientarse a evitar y atender el daño, no a la tecnología en sí misma. La IA no debe prohibirse en términos generales. Deben regularse los usos indebidos, como la desinformación, la manipulación, la opacidad, la afectación de derechos, el financiamiento ilícito, la propaganda encubierta o el daño a la integridad electoral. Esta distinción permite evitar respuestas dicotómicas y, al mismo tiempo, construir controles democráticos.

Conclusiones, propuestas y líneas de acción

La conclusión principal de la sede Morelia fue que la IA y las plataformas digitales deben incorporarse al análisis electoral como elementos estructurales de la contienda democrática. No se trata de fenómenos marginales ni de riesgos futuros. Ya inciden en la manera en que las personas se informan, opinan, se organizan, confían o desconfían, y definen su voto. Por ello, la justicia electoral debe desarrollar herramientas normativas, técnicas y pedagógicas para actuar antes de que el daño se vuelva irreversible.

Una vía de desarrollo consiste en regular la publicidad política digital. Debe construirse un marco que permita saber quién paga, cuánto paga, dónde se difunde, a qué audiencias se dirige, qué datos se utilizan y qué criterios de segmentación se

emplean. La propaganda digital no puede permanecer en una zona opaca en la que sea imposible distinguir el contenido espontáneo de la publicidad dirigida o de una campaña coordinada.

La agenda también exige establecer obligaciones de etiquetado para contenidos generados o modificados con IA. La ciudadanía debe saber si una imagen, un audio, un video o un texto fue producido mediante IA o alterado en grado sustancial. El etiquetado no supone prohibir el uso de IA; permite que las personas evalúen el mensaje con información suficiente. Esta medida es de especial relevancia cuando se trata de propaganda electoral o de contenidos relacionados con niñas, niños, candidaturas, autoridades o hechos verificables.

A ello hay que sumar el fortalecimiento de criterios sobre responsabilidad. Deben definirse reglas para determinar cuándo responde una candidatura, un partido, una plataforma, un proveedor tecnológico o una persona usuaria. La responsabilidad debe atender al grado de intervención: crear, pagar, coordinar, amplificar, beneficiarse, omitir el retiro de contenido ilícito o actuar con dolo. Sin reglas claras de imputación, las infracciones digitales pueden quedar impunes.

También resulta necesario desarrollar capacidades técnicas en las autoridades electorales. El Instituto Nacional Electoral (INE), los organismos públicos locales electorales (OPLE), los tribunales electorales y las áreas de fiscalización requieren equipos especializados en análisis digital, metadatos, redes, *bots*, pauta, IA generativa, *deepfakes*, procesamiento del lenguaje natural y preservación de evidencia. La prueba digital exige capacidades que no pueden improvisarse al momento de resolver.

Otra línea de acción es diseñar protocolos para contenidos sintéticos y *deepfakes*. Estos protocolos deben permitir una actuación rápida, medidas cautelares proporcionales, análisis técnico, preservación de evidencia y sanción cuando exista suplantación, falsedad intencional o afectación relevante a derechos y principios electorales. La rapidez es esencial porque el daño digital se produce y se multiplica antes de que concluya una investigación tradicional. En este trabajo es indispensable proteger la libertad de expresión mediante criterios diferenciados. La regulación no debe convertir al Estado en censor de toda opinión en redes. Debe distinguir entre ciudadanía y actores políticos, entre sátira y engaño, entre crítica y calumnia, entre error y dolo, entre contenido orgánico y campaña pagada, entre anonimato legítimo y redes coordinadas de manipulación. Sin estas distinciones, la respuesta puede ser excesiva o insuficiente.

La agenda regulatoria debe discutir mecanismos de verificación de identidad para contenidos de alto impacto. No se trata de eliminar el anonimato en internet, sino

de analizar si ciertos contenidos electorales, por su alcance, pauta, financiamiento o capacidad de afectar derechos, deben estar vinculados a sujetos identificables. La democracia requiere libertad, pero también rendición de cuentas.

A ello se agrega la posibilidad de utilizar IA para detectar riesgos. Las autoridades pueden apoyarse en algoritmos de detección, marcas de agua digitales, clasificadores de contenido, análisis de tendencias y herramientas de verificación. Sin embargo, estas herramientas deben operar con supervisión humana, transparencia, auditoría y respeto a los derechos, para evitar que la solución algorítmica reproduzca sesgos o genere nuevas formas de opacidad.

La transparencia es ahora, más que nunca, de enorme relevancia. Las plataformas deben informar sobre publicidad política, criterios de segmentación, reglas de moderación, retiro de contenidos, redes inauténticas, *bots*, cuentas coordinadas y mecanismos de atención a las autoridades electorales. Su poder en la conversación pública exige responsabilidades democráticas.

La regulación no puede depender solo del legislador ni solo de las plataformas. Es clave una gobernanza digital democrática que involucre a autoridades electorales, tribunales, universidades, especialistas en tecnología, sociedad civil, medios, partidos y ciudadanía. La complejidad del fenómeno exige respuestas interinstitucionales e interdisciplinarias.

Por último, se propone orientar el uso de IA hacia la mejora del debate público. La tecnología puede servir para verificar datos, comparar propuestas, analizar compromisos de campaña, traducir información, generar materiales accesibles y acercar la justicia electoral a la ciudadanía. La meta no debe ser expulsar la IA del proceso democrático, sino colocarla al servicio de una deliberación más informada y responsable. La sede Morelia aportó al recorrido regional una mirada ética, comunicativa y ciudadana sobre la IA electoral. Su contribución principal fue advertir que la tecnología no sustituye la responsabilidad democrática; la vuelve más urgente. En una época en la que no todo lo que se ve es real, la justicia electoral debe proteger no solo el resultado de la elección, sino las condiciones informativas que hacen posible una decisión libre, crítica y con autenticidad ciudadana.



San Francisco de Campeche, Campeche
Universidad Autónoma de Campeche



Contexto regional

En esta sede, el debate no se limitó a los riesgos generales de la tecnología en la comunicación política, sino que se orientó hacia preguntas más precisas: ¿qué límites puede imponer el Estado al uso de IA en contextos electorales?, ¿cuáles son los criterios más adecuados para sancionar la desinformación intencional?, ¿qué modelos regulatorios comparados ofrecen mejores herramientas?, y ¿qué capacidades institucionales necesita México para proteger la integridad democrática en la era algorítmica?

El contexto de Campeche tuvo un valor especial porque permitió articular varios planos de análisis. En el plano jurídico-comparado, la discusión revisó estándares interamericanos, experiencias latinoamericanas y modelos regulatorios como el europeo y el brasileño. En el plano tecnológico-operativo, se explicó cómo la microsegmentación, la recolección de datos, la ciberseguridad y el análisis en tiempo real pueden incidir en procesos electorales. En el plano ético-filosófico, se discutió qué debe ser la inteligencia artificial, cómo debe relacionarse con la actividad jurisdiccional y qué riesgos plantea para la autonomía ciudadana cuando adquiere apariencia de autoridad.

A diferencia de otras sedes, Campeche aportó una mirada muy marcada por la comparación internacional y por la necesidad de pasar de la preocupación general a la arquitectura institucional. La pregunta no fue solo si la IA puede ser peligrosa, sino qué herramientas concretas existen para enfrentarla: transparencia algorítmica, regulación de la publicidad política digital, identificación de anunciantes, marcas de agua, prohibición de la microsegmentación con datos sensibles, responsabilidad por riesgos sistémicos, multas a plataformas, desfinanciamiento de canales desinformativos, educación digital y pensamiento crítico.

La sede también permitió introducir un concepto de especial fuerza: el de autoridad sintética. La IA puede producir discursos coherentes, plausibles, bien redactados y en apariencia confiables, aunque no necesariamente verdaderos. Esa capacidad de generar apariencia de verdad puede inducir obediencia, confianza o persuasión en la ciudadanía frente a sistemas impersonales, opacos y manipulables. En materia electoral, el riesgo no es menor: una ciudadanía expuesta a discursos sintéticos puede tomar decisiones políticas a partir de información fabricada, mensajes dirigidos a influir en el plano emocional o contenidos con apariencias de neutralidad.

En conjunto, Campeche aportó al recorrido regional una mirada de regulación democrática. Su contribución principal fue advertir que la IA no puede abordarse solo como una herramienta tecnológica ni como una amenaza discursiva. Debe entenderse como un fenómeno capaz de afectar la libertad de expresión, la autonomía del voto, la equidad de la contienda, la integridad electoral, la impartición de justicia y la confianza pública. Por ello, la respuesta institucional debe ser preventiva, interdisciplinaria y cuidadosa desde el punto de vista constitucional.



Problemas o tensiones jurídicas

Un problema central fue la tensión entre la libertad de expresión y el combate a la desinformación. La mesa partió de los estándares interamericanos, tales como la prohibición de la censura previa, la neutralidad estatal frente a los contenidos, la protección del debate público y las obligaciones positivas del Estado para garantizar el pluralismo y el acceso a la información. Este punto es fundamental porque cualquier regulación de desinformación electoral puede convertirse, si se diseña mal, en una herramienta de censura. Al mismo tiempo, la ausencia absoluta de regulación permite que contenidos falsos, manipulados o coordinados afecten la formación libre de la voluntad ciudadana.

Otra tensión, como en otras mesas, fue la insuficiencia del marco jurídico mexicano. Aunque existen principios constitucionales aplicables, criterios jurisdiccionales y algunos lineamientos, todavía no hay una regulación integral sobre IA, publicidad política digital, microsegmentación y plataformas en procesos electorales. La mesa recordó que en algún momento se discutió la posibilidad de reformar el artículo 41 constitucional para identificar contenidos generados por IA y *deepfakes* electorales, pero esa propuesta no prosperó. La consecuencia es que los operadores jurídicos

deben resolver con normas generales asuntos que tienen una especificidad tecnológica muy alta.

Cuando circula un contenido falso o manipulado con IA, no siempre es claro quién debe responder: quien lo creó, quien lo difundió, quien pagó la pauta, quien se benefició en el plano electoral, la plataforma que lo amplificó o el proveedor tecnológico que permitió su generación. Esta no es una cuestión menor: la definición de la cadena de responsabilidades en el proceso de comunicación digital. La experiencia comparada muestra respuestas distintas: sancionar a los usuarios, sancionar a partidos y candidaturas, exigir cuentas a plataformas o perseguir redes coordinadas de desinformación. Campeche mostró que una mala asignación de responsabilidades puede producir dos riesgos opuestos: la impunidad o la sobrerregulación.

A ello se sumó la diferencia entre regular contenidos y regular infraestructura. El modelo de control social sanciona la emisión o difusión de contenidos, con riesgos evidentes para la libertad de expresión. En cambio, los modelos de auditoría a *gatekeepers* y de desarticulación de redes se concentran en plataformas, publicidad, algoritmos, financiamiento, redes coordinadas y riesgos sistémicos. La mesa sugirió que la pregunta estratégica no debe ser solo qué contenido se elimina, sino ¿quién lo financia?, ¿cómo se amplifica?, ¿por qué se muestra a ciertos grupos? y ¿qué responsabilidades tienen las plataformas que estructuran la conversación pública?

Una preocupación que propició un consenso entre las personas participantes del diálogo fue el desfase entre capacidad institucional y sofisticación tecnológica. La mesa fue clara: no basta con almacenar información electoral; es necesario analizarla. Las instituciones cuentan con grandes volúmenes de datos, pero no siempre los utilizan para detectar patrones anómalos, campañas coordinadas, manipulación informativa o riesgos en tiempo real. La amenaza tecnológica exige capacidad tecnológica, analítica y humana. Sin esas tres dimensiones, la respuesta institucional será tardía.

Otro aspecto relevante fue la relación entre IA y jurisdicción, en el contexto de la regulación europea, que considera la impartición de justicia como actividad de alto riesgo si depende en alguna etapa de su proceso en un modelo de IA. La mesa enfatizó que la adjudicación debe recaer en personas naturales, tanto en la investigación de hechos como en la interpretación de normas. La IA puede auxiliar, sistematizar, buscar o clasificar información, pero no debe sustituir la responsabilidad humana de juzgar. Este principio también se proyecta a mecanismos alternativos de solución de controversias, como el arbitraje.

Respecto a la dificultad para sancionar la desinformación intencional, se discutió la doctrina de la real malicia, según la cual no basta con que la información sea falsa, sino que debe acreditarse que el emisor sabía que era falsa o actuó con desprecio temerario por la verdad. En materia electoral, esta doctrina puede ser útil, pero insuficiente si no existe un tipo legal o constitucional que permita sancionar. La legalidad exige bases normativas claras; sin ellas, incluso una conducta dañina puede quedar fuera del alcance sancionador.

Asimismo, la mesa recuperó experiencias en las que una autoridad nacional intenta vincular a una plataforma y esta no responde, no se da por notificada o no cumple. El problema no es solo jurídico, sino también de una relación de poder carente de controles suficientes. Las plataformas digitales operan a escala global, concentran datos, controlan algoritmos, administran publicidad y deciden condiciones de visibilidad. Sin órganos garantes fuertes, representación local efectiva, cooperación internacional y sanciones ejecutables, muchas decisiones electorales pueden volverse simbólicas.

Al cierre, se identificó una tensión entre el pensamiento crítico y la manipulación algorítmica. Una intervención del público señaló que las redes sociales aglomeran preferencias afines, bloquean perspectivas contrarias y reducen la capacidad de visión amplia. La microsegmentación no solo dirige mensajes; también puede restringir el horizonte de información disponible para cada persona. Por ello, la defensa democrática no puede depender solo de reglas jurídicas. Requiere una ciudadanía capaz de cuestionar, verificar, contrastar y romper cercos informativos.



Aportes conceptuales

Otro aporte conceptual de especial relevancia de Campeche fue la distinción entre regulación democrática y control autoritario. No toda regulación de desinformación es deseable. Los modelos de control social, asociados a leyes que criminalizan contenidos, incautan equipos o sancionan difusión ciudadana, muestran el riesgo de utilizar la lucha contra la desinformación como excusa para controlar a los medios y a la ciudadanía. La regulación democrática debe evitar ese camino y concentrarse en transparencia, rendición de cuentas, publicidad política, plataformas y redes coordinadas de manipulación.

En esta línea, se abonó al diálogo el concepto de *gatekeepers*. Las grandes plataformas digitales funcionan como guardianes de la conversación pública, deciden qué

se muestra, a quién, cuándo, con qué prioridad y con qué lógica algorítmica. Por ello, la regulación electoral no puede limitarse a partidos y candidaturas. Debe incluir obligaciones de transparencia, auditoría, trazabilidad y rendición de cuentas para quienes administran la infraestructura digital del debate público.

También destacó la idea de riesgos sistémicos para la democracia. ¿A qué se refiere este apunte? La clave es entender que no todos los daños digitales se reducen a una publicación específica; puede haber también dinámicas amplias de manipulación, redes automatizadas, publicidad opaca, microsegmentación masiva, financiamiento encubierto, desinformación coordinada y algoritmos que amplifican la polarización. En esos casos, la responsabilidad no debe analizarse solo publicación por publicación, sino también desde la perspectiva de los riesgos estructurales o sistémicos para la integridad democrática.

La mesa fue contundente: sin regular la publicidad, no es posible regular la desinformación. Si no se sabe quién paga, cuánto paga, qué contenido difunde, a quién lo dirige y con qué segmentación, la autoridad no puede reconstruir el circuito de influencia. La transparencia publicitaria es una condición mínima para fiscalizar las campañas digitales.

Un concepto novedoso fue la autoridad sintética. Esto, en el sentido de que la IA puede generar discursos con apariencia de coherencia, neutralidad y verdad. Esa plausibilidad puede ser confundida con conocimiento. En democracia, este fenómeno es peligroso porque una herramienta artificial puede adquirir autoridad persuasiva sin responsabilidad, sin conciencia, sin compromiso con la verdad y sin rendición de cuentas. La ciudadanía puede otorgar credibilidad a una voz que no es humana ni institucional, pero que parece confiable.

Ahora bien, frente a la manipulación digital, la mesa propuso avanzar hacia una democracia epistémica y dialógica, basada en el pensamiento crítico, la identificación de falacias, el reconocimiento de sesgos algorítmicos y la apertura a puntos de vista distintos. Esta propuesta amplía la discusión: no basta defender el voto; hay que defender las condiciones de conocimiento que permiten votar con libertad.

Una contribución creativa e incluso lúdica fue trabajar en una redefinición de la ética respecto a la IA, pero no desde cero, sino mediante la aplicación de los principios ya existentes de forma creativa y juiciosa. La IA debe estar centrada en la persona humana, respetar los derechos fundamentales, proteger la democracia y el Estado de derecho y evitar formas de manipulación subliminal o interferencia en las motivaciones de las personas.

Por otra parte, el diálogo dejó claro que ya no basta con abogados electorales ni con un equipo ínfimo de ingenieros en sistemas. Se necesitan instituciones con infraestructura tecnológica, ciberseguridad, análisis en tiempo real, personal especializado, formación académica, alfabetización digital, cooperación con universidades y capacidad de respuesta frente a ataques automatizados. La justicia electoral del futuro será necesariamente interdisciplinaria.

Por último, se propuso una estrategia, no excluyente de otras, pero que siempre ha sido funcional en el mundo electoral: seguir el dinero. La manipulación digital suele estar asociada a intereses económicos, pauta, financiamiento, publicidad, contratación de servicios, *influencers*, plataformas y redes de amplificación. La ruta del dinero puede revelar quién impulsó un contenido, quién se benefició y quién debe responder. En campañas digitales, la fiscalización debe mirar tanto el mensaje como su financiamiento.



Conclusiones, propuestas y líneas de acción

Un eje de trabajo consiste en regular la publicidad política digital. Debe exigirse la identificación de anunciantes, los montos invertidos, el contenido difundido, los criterios de segmentación, las audiencias objetivo y las personas responsables de contratación. La fiscalización electoral debe poder rastrear los recursos en entornos digitales, incluyendo publicidad en plataformas, *influencers,* buscadores, mensajería, redes sociales y servicios de segmentación.

Otro paso consiste en establecer obligaciones de transparencia algorítmica para las grandes plataformas. Aunque la transparencia algorítmica es un concepto complejo, debe traducirse en obligaciones concretas: reportes de funcionamiento, criterios de recomendación, políticas de moderación, bibliotecas de anuncios, auditorías independientes, evaluación de riesgos y explicación de decisiones que afecten contenidos político-electorales.

A ello se suma la necesidad de prohibir o limitar de manera estricta la microsegmentación con datos sensibles en campañas electorales. La orientación política, la religión, el origen étnico, la salud, la discapacidad, la ubicación precisa, las emociones o las vulnerabilidades personales no deben utilizarse para manipular la voluntad ciudadana. Debe discutirse, incluso, si la microsegmentación electoral debe prohibirse en términos generales para recuperar un debate público compartido.

La agenda puede complementarse con la incorporación de marcas de agua o mecanismos de identificación de contenido generado con IA. Las empresas desarrolladoras, las plataformas y los actores políticos deben facilitar la detección de contenido sintético. Además, los partidos y las candidaturas deberían informar al INE cuando usen contenido generado con IA y reportar los gastos correspondientes para efectos de fiscalización.

Conviene crear también capacidades institucionales de ciberseguridad y análisis en tiempo real. Las autoridades electorales necesitan monitorear ataques automatizados, campañas coordinadas, patrones de desinformación, anomalías en datos electorales y manipulación digital. No basta con conservar bases de datos; deben analizarse de forma sistemática para identificar riesgos a tiempo.

Es indispensable fortalecer la alfabetización digital y el pensamiento crítico. La ciudadanía debe aprender a identificar falacias, sesgos, *deepfakes*, contenidos sintéticos, publicidad segmentada y manipulación emocional. Esta formación debe incluir a escuelas, universidades, campañas públicas, autoridades electorales, partidos y medios. Una democracia vulnerable en el plano cognitivo es una democracia vulnerable en el plano electoral.

Otra ruta de trabajo apunta a preservar la decisión jurisdiccional humana. La IA puede ser una herramienta auxiliar para la búsqueda, la sistematización o el análisis, pero no debe sustituir a las personas juzgadoras. Las decisiones que afectan derechos políticos, resultados electorales, libertad de expresión o sanciones deben recaer en autoridades humanas responsables, con motivación jurídica y rendición de cuentas.

A ello se agrega la necesidad de construir tipos normativos claros para sancionar la desinformación electoral intencional. La sanción debe cumplir con el principio de legalidad. Para evitar la arbitrariedad, debe definirse qué conductas son ilícitas: suplantación de identidad, *deepfakes* no identificados, desinformación deliberada con capacidad de afectar el voto, uso de *bots*, financiamiento opaco, manipulación con datos sensibles o incumplimiento de obligaciones de transparencia.

También debe avanzarse en el establecimiento de criterios de responsabilidad por riesgos sistémicos. Cuando una plataforma, una red de actores o una campaña digital comprometa la integridad democrática mediante prácticas coordinadas, no debe analizarse solo una publicación aislada. Debe evaluarse el riesgo sistémico producido y la responsabilidad de quienes permitieron, financiaron o amplificaron la operación.

La agenda también incluye establecer medidas frente a los fenómenos de viralización. Cuando un contenido desinformativo o manipulado sea identificado conforme a

reglas claras, deben existir herramientas proporcionales para reducir su circulación: etiquetado, desmonetización, limitación de reenvíos, suspensión de pauta, preservación de evidencia y, en casos graves, retiro. Estas medidas deben aplicarse con garantías, motivación y control posterior.

Además, conviene fortalecer la cooperación con las plataformas globales bajo un paradigma clave: no es una relación entre iguales; el Estado es responsable de proteger la libertad de expresión, así como las condiciones de la conversación pública. Las autoridades mexicanas necesitan canales de notificación eficaces, representación local, plazos de respuesta, cumplimiento de órdenes, protocolos de evidencia y sanciones ejecutables. Una orden electoral que una plataforma ignora debilita la autoridad del Estado y la confianza en la justicia.

Otra propuesta consiste en promover investigación y desarrollo tecnológico con enfoque democrático. Ideas como la de una urna electrónica con IA, las interfaces en lenguas originarias y el diseño inclusivo muestran que la tecnología también puede ampliar el acceso y la participación. Las universidades pueden desempeñar un papel estratégico en innovación pública, siempre que se garanticen el secreto del voto, la seguridad, la auditabilidad, la accesibilidad y la confianza.

Recapitulando, la sede Campeche aportó al recorrido regional una mirada regulatoria, comparada y ética. Su contribución principal fue advertir que la democracia mexicana no puede esperar a que la manipulación digital produzca daños irreversibles. Debe actuar antes, con reglas claras, capacidades técnicas, pensamiento crítico, transparencia publicitaria, supervisión de plataformas y una convicción de fondo: la tecnología debe estar al servicio de la ciudadanía, no de su manipulación.

Tlaxcala de Xicohténcatl, Tlaxcala
Universidad Autónoma de Tlaxcala



Contexto regional

A esas alturas del recorrido nacional, la discusión sobre IA partió de su reconocimiento como un fenómeno presente que atraviesa la vida cotidiana, la investigación jurídica, la comunicación política, la fiscalización electoral, la formación de la voluntad ciudadana y la propia función jurisdiccional.

La sede tlaxcalteca aportó una mirada de especial relevancia porque la conversación se desarrolló en un espacio universitario con fuerte tradición en filosofía del derecho, argumentación jurídica y justicia electoral. Ello permitió que el debate no se concentrara solo en los riesgos externos de las plataformas digitales durante las campañas, sino también en una pregunta más profunda: ¿cómo debe relacionarse el derecho con la IA cuando esta comienza a intervenir en la forma en que los individuos argumentan, deciden, sienten y piensan?

Tlaxcala aportó, además, un énfasis particular: la IA no debe entenderse solo como una amenaza para las elecciones, sino también como una herramienta que ya forma parte del trabajo jurídico ordinario. Profesores, estudiantes, litigantes, personas servidoras públicas y órganos jurisdiccionales utilizan o enfrentarán el uso de modelos generativos. El problema no es impedir su uso, sino evitar que su incorporación superficial produzca razonamientos débiles, citas inexistentes, argumentos aparentes, falsas inferencias o decisiones sin control humano suficiente.

La sede también permitió vincular la discusión tecnológica con preguntas de legitimidad democrática. En una época de campañas algorítmicas, la ciudadanía ya no recibe solo mensajes políticos generales, como ocurría con la radio y la televisión. Recibe contenidos personalizados, filtrados por algoritmos y

diseñados a partir de datos personales, preferencias, emociones, hábitos de consumo y comportamiento digital. Esto modifica la estructura misma del debate público: cada persona puede quedar encerrada en una burbuja informativa en la que solo aparecen mensajes compatibles con sus creencias previas. Su contribución principal fue mostrar que la IA también transforma las condiciones de producción del conocimiento jurídico, la formación de la voluntad ciudadana y la capacidad institucional para distinguir entre realidad, simulación, manipulación y prueba.



Problemas o tensiones jurídicas

Un problema central fue la falta de una conciencia regulatoria integral. Desde la presentación inicial se señaló que México aún no ha desarrollado por completo un marco que atienda la importancia de regular los mecanismos presentes en las plataformas digitales y, en particular, la IA. La regulación existente ha sido segmentada, reactiva y fragmentaria, mientras que el fenómeno tecnológico es global, transversal y acelerado. Esta brecha genera un problema estructural: la IA opera sin fronteras, pero las respuestas jurídicas siguen organizadas desde marcos nacionales y sectoriales muchas veces insuficientes.

Se identificó también la insuficiencia del llamado "*prompt* jurídico" —instrucción que se da a los modelos de IA generativa, como *chatbots*, para obtener respuestas— como solución. La mesa sostuvo que no basta con aprender instrucciones superficiales para obtener mejores respuestas jurídicas de una IA. El uso serio de estas herramientas exige un marco metodológico, teoría de la argumentación, teoría de la prueba, identificación de sesgos, control de inferencias, revisión de fuentes, comprensión del problema jurídico y responsabilidad profesional. Sin ese marco, la IA puede condicionar la forma en que abogados, estudiantes o personas juzgadoras interpretan, argumentan y resuelven problemas, en lugar de servir como herramienta auxiliar.

Un tema que adquirió especial relevancia fue la ciberseguridad institucional. La mesa advirtió que la manipulación digital del voto no se limita a la propaganda o la desinformación. También involucra la protección de servidores, bases de datos, sistemas de gobierno, plataformas electorales, información personal y servicios públicos. Se planteó la necesidad de invertir en ciberseguridad, pruebas de penetración, prevención de ataques, capacitación especializada y mecanismos de respuesta frente a amenazas complejas. La confianza electoral en la era digital depende tanto de la integridad

del discurso público como de la seguridad de la infraestructura tecnológica. En este sentido, el Estado mexicano debe tener claros los riesgos que representan los actores no tradicionales y reconocer que las amenazas digitales provienen ahora de grupos cibercriminales, empresas, gobiernos extranjeros, redes automatizadas, *bots*, granjas de cuentas o incluso sistemas de IA diseñados para detectar vulnerabilidades. Esta pluralidad de actores dificulta la atribución de responsabilidades y exige capacidades institucionales nuevas. El modelo clásico de infractor individual resulta insuficiente frente a redes distribuidas y operaciones transnacionales.

Otro aspecto relevante fue la propaganda generada con IA y el interés superior de la niñez. La mesa retomó el precedente de propaganda política en la que se utilizó una imagen de un niño generada por IA; la discusión mostró una pregunta delicada: si no existe un niño real, ¿hay afectación al interés superior de la niñez? Desde una lectura de forma estrictamente individual, podría decirse que no se vulnera la imagen de una persona identificable. Sin embargo, desde la percepción ciudadana, una imagen sintética puede generar los mismos efectos emocionales que una imagen real. Esto obliga a repensar las categorías de consentimiento, imagen, representación simbólica y manipulación emocional.

En algún punto, la mesa abordó la nueva causal de nulidad por intervención o injerencia extranjera, recién aprobada por la reforma electoral de 2026. El diálogo vinculó este tema con el caso rumano, en el que se anuló una elección presidencial por una campaña coordinada mediante plataformas digitales, TikTok, *bots*, cuentas falsas, redes de amplificación e *influencers*. La pregunta jurídica es compleja: ¿cómo acreditar una intervención extranjera cuando la IA y las plataformas difuminan fronteras, ocultan el origen, multiplican intermediarios y permiten operar desde entornos distribuidos? La prueba de gravedad, dolo, determinancia y responsabilidad se vuelve especialmente difícil.

En la era de las campañas algorítmicas, no siempre es sencillo distinguir entre expresión ciudadana, contenido orgánico, publicidad encubierta, pago a *influencers*, operación coordinada o gasto de campaña. El modelo de comunicación política, diseñado para un ecosistema de radio, televisión y propaganda más visible, resulta insuficiente frente a redes sociales, pauta digital, contenidos virales, algoritmos y financiamiento indirecto. La fiscalización necesita trazabilidad, seguimiento de recursos y reglas específicas para plataformas.



Aportes conceptuales

Un aporte relevante fue la necesidad de una gobernanza institucional de la IA en la impartición de justicia. La incorporación de IA al trabajo jurisdiccional requiere más que entusiasmo tecnológico. Necesita juntas o comités de gobierno, especialistas, protocolos, marcos normativos, capacitación, criterios de uso, supervisión humana y evaluación constante. Sin gobernanza, la adopción de IA puede producir prácticas fragmentadas o improvisadas y generar riesgos de legitimidad.

Otra contribución relevante fue la noción de burbuja informativa como problema democrático. Los algoritmos tienden a mostrar más de aquello que confirma gustos, intereses o creencias previas de las personas usuarias. Esto puede reducir la exposición a puntos de vista divergentes, empobrecer el debate público y aumentar la polarización. Una ciudadanía encerrada en burbujas informativas puede creer que su percepción parcial de la realidad representa la totalidad del debate democrático.

Una novedad fue la lectura de la microsegmentación algorítmica en clave del libre desarrollo de la personalidad. En el diálogo se planteó que las plataformas construyen perfiles artificiales o sociales de las personas, a partir de datos que muchas veces no controlan por completo. Esta construcción claramente puede incidir en sus decisiones, consumos, opiniones y preferencias políticas. La protección de la autonomía personal exige pensar los datos y los algoritmos no solo como herramientas comerciales, sino como dispositivos que afectan la libertad, la identidad y la participación pública.

En algún punto del diálogo se incorporó un aspecto no menor: el desafío supranacional. Es decir, la discusión subrayó que la IA no reconoce fronteras nacionales. Las plataformas operan a escala global; los datos circulan en el plano internacional; los servidores pueden estar en otro país, y la influencia política puede organizarse desde redes transnacionales. Por ello, la regulación de plataformas e IA quizá deba pensarse como parte de una agenda pública global, comparable a otros problemas transnacionales —como el cambio climático o el armamento nuclear— que exceden la capacidad de los Estados para actuar de forma aislada.

Conclusiones, propuestas y líneas de acción

La principal conclusión de la sede Tlaxcala fue que la IA llegó para quedarse y que la justicia electoral debe aprender a trabajar con ella sin renunciar a sus principios. El reto no es prohibir toda innovación ni aceptar acríticamente su expansión. El desafío es construir una relación institucional inteligente: aprovechar sus beneficios, controlar sus riesgos, preservar la decisión humana y proteger la democracia frente a nuevas formas de manipulación.

Es indispensable, a su vez, incluir en la agenda regulatoria marcos metodológicos para el uso de IA en la justicia electoral. Las personas juzgadoras, secretarias, proyectistas, litigantes y académicas deben contar con criterios claros sobre qué puede hacerse con IA, qué no debe delegarse, cómo verificar los resultados, documentar su uso y evitar sesgos o errores. La IA debe auxiliar la labor jurisdiccional, no sustituir la responsabilidad de razonar y decidir.

Una línea de trabajo clave es diseñar protocolos institucionales de gobernanza de la IA. Las autoridades electorales y jurisdiccionales deben establecer órganos o comités especializados, reglas internas, auditorías, controles de calidad, políticas de protección de datos, criterios de transparencia y mecanismos de supervisión humana. Sin protocolos, el uso de IA puede depender de prácticas individuales y generar desigualdad o riesgos de legitimidad.

Otra propuesta apunta a regular la propaganda generada con IA, en especial cuando involucre a la niñez, personas candidatas, autoridades o grupos vulnerables. Todo contenido sintético debe identificarse como tal cuando pueda afectar la percepción ciudadana. En el caso de niñas, niños y adolescentes, debe considerarse no solo si existe una persona real identificable, sino también los efectos emocionales, simbólicos y políticos de utilizar imágenes infantiles artificiales en campaña.

Es importante que se legisle con claridad en cuanto a la causal de nulidad por intervención extranjera digital. Al incorporarse como causal de nulidad la injerencia extranjera, deben definirse aspectos como los estándares probatorios adecuados, qué cuenta como intervención, cómo se acredita el origen, la coordinación, el financiamiento, la gravedad, el dolo y el impacto. Sin reglas claras, la causal puede ser simbólica o, en el extremo opuesto, susceptible de manipulación política.

A partir de la mesa de Tlaxcala, un punto queda claro: la democracia digital requiere instituciones inteligentes y ciudadanía crítica. La IA puede fortalecer el acceso a

la justicia, mejorar procesos, ampliar capacidades y democratizar el acceso a la información. Pero también puede inventar, manipular, segmentar, suplantar y erosionar la confianza. La diferencia dependerá de la calidad de las reglas, de las instituciones y de la cultura democrática. Por ello, es importante advertir que el desafío no consiste solo en regular las plataformas o sancionar la desinformación, sino en formar operadores jurídicos, autoridades y ciudadanía capaces de gobernar la tecnología sin ser gobernados por ella. La justicia electoral cercana, en la era de la IA, debe ser también una justicia sólida en el plano argumentativo, preparada desde el punto de vista técnico y comprometida con la democracia.

Ciudad de México
Universidad Autónoma Metropolitana
Rectoría General



Contexto regional

La Ciudad de México concentra autoridades electorales nacionales y locales, órganos jurisdiccionales, academia especializada, sociedad civil, empresas tecnológicas, medios de comunicación, organizaciones políticas y una ciudadanía intensamente conectada a plataformas digitales. Por ello, la conversación no se desarrolló solo desde una perspectiva abstracta sobre IA, sino desde la experiencia concreta de quienes enfrentan en la vida cotidiana los dilemas de moderación de contenidos, solicitudes de retiro, violencia política digital, fiscalización de anuncios, interacción con plataformas privadas, capacitación institucional y control jurisdiccional.

La discusión se abrió con las preguntas detonadoras que guiaron todo el volumen: ¿cómo impactan la tecnología y la IA en la labor jurisdiccional electoral? ¿Cuál debe ser el alcance del control jurisdiccional sobre plataformas privadas? ¿Qué límites deben aplicarse a la propaganda política generada mediante IA? ¿Cuáles son los criterios para sancionar la desinformación intencionada? ¿Cómo afecta la microsegmentación política a la igualdad de la contienda? ¿Qué capacidades institucionales requiere el Estado para enfrentar la manipulación digital del voto?

La sede capitalina aportó así una dimensión particularmente técnica e institucional. Mientras otras sedes habían enfatizado riesgos como *deepfakes*, microsegmentación o alfabetización digital, la Ciudad de México permitió profundizar en la arquitectura de las plataformas, la economía de la atención, los límites del modelo de comunicación política del artículo 41 constitucional, la necesidad de regulación, la relación entre autoridades electorales y empresas tecnológicas, y los desafíos probatorios de

fenómenos como *bots*, *astroturfing* y comportamiento inauténtico coordinado. Su contribución principal fue advertir el papel de las infraestructuras privadas extranjeras que seleccionan, ordenan, amplifican, reducen, etiquetan o retiran contenidos políticos, conforme a los parámetros de sus propios modelos de negocio. La justicia electoral cercana, en este contexto, debe ser capaz de dialogar con esas infraestructuras sin subordinarse a ellas, al tiempo que exige reglas compatibles con la libertad de expresión, la equidad, la autenticidad del voto y el ejercicio de la soberanía democrática.



Problemas o tensiones jurídicas

Un problema central fue la insuficiencia del modelo constitucional de comunicación política frente al ecosistema digital. El diseño del artículo 41 constitucional y de la reforma electoral de 2007-2008 fue construido, sobre todo, para radio, televisión, propaganda impresa, espectaculares y medios tradicionales. Este modelo permite identificar con relativa claridad al emisor, el contenido difundido, el tiempo de transmisión, el gasto y la audiencia potencial. Sin embargo, las plataformas digitales operan bajo otra lógica: contenidos personalizados, anuncios segmentados, mensajes orgánicos, cuentas automatizadas, *influencers*, publicidad encubierta, algoritmos de recomendación y circulación transfronteriza.

Otra tensión fue la asimetría regulatoria entre medios tradicionales y plataformas digitales. Mientras la radio y la televisión están sometidas a un régimen constitucional y administrativo robusto, las redes sociales funcionan en buena medida bajo políticas privadas, términos de servicio, memorándums de entendimiento, acuerdos de colaboración y canales de comunicación institucional. La mesa identificó que el control jurisdiccional actual sobre las plataformas es indirecto, casuístico, con una orientación en buena medida *ex post* y dependiente de la existencia de un caso concreto. Esto limita la capacidad de prevenir daños sistémicos durante las campañas.

También se discutió la relación entre la libertad de expresión y la integridad electoral. La representante de la empresa Meta, quien participó en la mesa, argumentó que las plataformas de esta empresa han permitido expandir la libertad de expresión y la conversación pública. No obstante, la discusión dejó claro que no se debe confundir la libertad de expresión con el modelo de negocio de las plataformas ni permitir que la alusión a la libertad de expresión pueda usarse como ardid para posibilitar la difusión

de desinformación, violencia, suplantación de identidad, cuentas falsas, *deepfakes*, manipulación o interferencia electoral.

Asimismo, se problematizó el uso y la explotación indiscriminados de la información personal de las y los usuarios —sin conocimiento— por parte de las plataformas como modelo de negocios que contribuye a la propagación de las malas prácticas antes indicadas. En este sentido, se habló de las problemáticas para distinguir el contenido legítimo, la crítica política, la sátira, el error y la opinión, de la propaganda, la desinformación intencionada y la manipulación coordinada. Si bien una regulación excesiva podría derivar en censura, una regulación insuficiente permite que la mentira y la desinformación intencionada y planificada condicionen la conversación pública.

La representante de Meta indicó que, en plataformas utilizadas por miles de millones de personas, la revisión humana integral resulta imposible; de ahí la necesidad de sistemas automatizados de detección, moderación y priorización. Sin embargo, esta solución generó nuevas preguntas que se indicaron en la mesa, preguntas relativas a quién define las reglas, con qué criterios se entrena la IA, cómo se evitan errores, qué contenidos se bajan de forma automática, cómo se corrigen decisiones equivocadas y qué grado de transparencia debe exigirse a las plataformas. La discusión de los temas apuntó a que la moderación algorítmica es necesaria y no puede ser opaca.

La mesa abordó, a su vez, la eliminación masiva de cuentas falsas, la detección de patrones anómalos, el comportamiento inauténtico coordinado y la dificultad para identificar cuándo una interacción digital corresponde a una persona real, a una red de *bots*, a cuentas automatizadas o a una operación organizada. Este punto es central para la materia electoral: la deliberación democrática presupone que las voces públicas corresponden, en principio, a la ciudadanía, los medios, los actores políticos o las instituciones identificables, no a una simulación artificial de apoyo social.

Además, se observó la fiscalización de la publicidad política digital. La representante de Meta expuso la existencia de bibliotecas de anuncios, procesos de identificación de anunciantes, *disclaimers* sobre quién paga y datos sobre el alcance, el costo, la temporalidad y la ubicación. Estos mecanismos pueden ser útiles para la fiscalización electoral, en especial cuando permiten reconstruir quién contrató, cuánto pagó, dónde se difundió y a quién alcanzó un anuncio. Sin embargo, la mesa también evidenció que estos mecanismos dependen, en buena medida, de reglas internas de plataformas y no de un marco legal mexicano integral que obligue a todas ellas por igual.

Un tema en particular relevante que se presentó en la conversación es el control jurisdiccional sobre plataformas privadas. La mesa reconoció que existen antecedentes

de colaboración, como el memorándum entre Facebook y el INE o instrumentos de entendimiento con otras plataformas, pero también se señaló que esos mecanismos no tienen fuerza de ley ni aseguran una respuesta uniforme de todas las empresas. El problema se agrava cuando las empresas que manejan las plataformas digitales son renuentes a atender solicitudes de las autoridades, cuando no existe representación local suficiente o cuando las órdenes electorales dependen de estándares privados de cumplimiento.

La violencia política digital contra las mujeres se presentó como otro elemento importante. Desde la experiencia de las autoridades locales se planteó la necesidad de contar con mecanismos más ágiles para bajar contenidos, retirar páginas que difunden violencia de forma sistemática, capacitar a las candidaturas en autoprotección digital y evitar que todo dependa de procedimientos largos. El problema no es solo retirar una publicación aislada, sino atender páginas, perfiles o campañas construidas para violentar de forma recurrente a mujeres en política. La discusión mostró que la coordinación entre plataformas, INE, OPLE, tribunales locales y candidaturas debe fortalecerse y que deben existir mecanismos legales que no dejen la respuesta a los casos concretos al arbitrio de la empresa controladora de la plataforma.

Como cierre, se identificó una tensión en torno a la verdad en la democracia. Se subrayó que la próxima gran disputa de las autoridades electorales será contra la mentira, la manipulación y la falsedad organizada. La verdad no fue entendida como una categoría abstracta, sino como condición de la decisión y de la vida democrática. Una ciudadanía que vota con información falsa, con mensajes personalizados en el plano emocional o con información manipulada y amplificada mediante IA, no decide en condiciones de libertad.



Aportes conceptuales

Un aporte conceptual de especial importancia de la sede Ciudad de México fue distinguir entre algoritmo, sistema algorítmico e IA. Esta precisión permite evitar diagnósticos equivocados. El algoritmo no es una voluntad autónoma, sino una cadena de procedimientos programados que seleccionan y ordenan contenidos conforme a ciertos objetivos definidos por seres humanos. La IA, por su parte, no es conciencia ni deliberación humana, sino un conjunto de modelos especializados que predicen, clasifican y generan resultados a partir de ciertas metas trazadas previamente, en función de la cantidad y calidad de datos proporcionados.

Fue importante que se concluyera que las plataformas en línea operan bajo objetivos de negocio. De ahí que la organización del contenido, en el mundo digital, no responda en primera instancia a valores democráticos. Más bien, se organiza a partir de métricas de tiempo de visualización, interacción, permanencia, retención, cantidad de clics y viralidad del contenido, entre otras más, con un fines publicitarios y lucrativos. Este punto es crucial para la justicia electoral: la infraestructura en la que ocurre buena parte de la deliberación democrática está optimizada, en buena medida, por incentivos comerciales.

Una distinción relevante, propia de la democracia moderna, fue la establecida entre desinformación y simple error. Desde la perspectiva de la plataforma, puede ser relevante retirar información errónea o reducir su difusión aun sin acreditar dolo cuando cause daño, riesgos a la salud o interferencia electoral. En cambio, desde la perspectiva jurisdiccional, la intencionalidad resulta relevante para graduar la responsabilidad. Esta distinción muestra que los estándares de moderación privada y los estándares jurídicos de sanción no son idénticos, aunque deban dialogar entre sí.

Otra contribución fue el papel de las bibliotecas de anuncios o pautas de los intermediarios en línea. La publicidad política digital requiere trazabilidad: quién paga, cuánto paga, cuándo circula, en qué entidad se muestra, a cuántas personas alcanza y con qué criterios de segmentación. La biblioteca de anuncios, en este sentido, puede funcionar como instrumento de fiscalización, prueba y rendición de cuentas. La sede metropolitana mostró que la transparencia publicitaria no es un accesorio, sino una condición mínima para controlar campañas digitales.

Otra categoría que se planteó fue la de comportamiento inauténtico coordinado. Es decir, la manipulación electoral digital no siempre consiste en una publicación falsa; también puede consistir en redes de páginas, cuentas o perfiles que simulan apoyo ciudadano, se presentan como medios informativos, amplifican narrativas o coordinan interacciones. Este fenómeno exige analizar patrones, no solo contenidos individuales.

La mesa hizo hincapié en el fenómeno de *astroturfing* como un mecanismo que genera falsa organicidad de los contenidos digitales. Se explicó que ciertos movimientos digitales pueden aparentar apoyo ciudadano de base, cuando en realidad son operaciones propagandísticas infladas mediante IA, *bots*, cuentas coordinadas, contenido generado con IA y que están financiadas de forma opaca. En materia electoral, este fenómeno puede alterar la percepción de viabilidad, popularidad o rechazo de candidaturas y gobiernos.

A ello se agregó la necesidad de entender la prueba digital como prueba contextual y técnica. La discusión subrayó que no basta con una impresión subjetiva para afirmar que hay *bots*, *deepfakes* o manipulación. Se requieren análisis técnicos, contexto, patrones, metadatos, bibliotecas de anuncios, fuentes verificables y valoración jurídica. A la vez, se debe evitar que la exigencia probatoria se convierta en una barrera irrazonable para quienes denuncian violencia o desinformación.

En esta mesa se insistió en la centralidad de la verdad como condición democrática. La sede de la Ciudad de México recuperó una preocupación transversal, propia de otros seminarios, relativa a que la ciudadanía necesita información útil, oportuna, fidedigna y plural para votar con responsabilidad. La mentira digital es un problema de contenido y una vulneración a los derechos de ciertas personas, pero también es una afectación al proceso de formación de la voluntad política.

Por último, se destacó el reconocimiento de que los modelos regulatorios comparados deben estudiarse con sentido crítico. Se mencionaron como referentes a la Unión Europea y Brasil. Sin embargo, también se advirtió que México no debe copiar de forma mecánica normas extranjeras, sino analizar sus efectos, evitar redundancias, aprender de sus resultados y adaptar cualquier modelo a la realidad nacional, al sistema electoral mexicano y a sus principios constitucionales.



Conclusiones, propuestas y líneas de acción

Un campo de trabajo urgente consiste en actualizar el modelo de comunicación política. El diseño vigente, centrado en radio y televisión, resulta insuficiente para enfrentar la publicidad digital, contenido orgánico amplificado, microsegmentación, *influencers*, *deepfakes*, *bots* y campañas coordinadas. La reforma no debe abandonar los principios del artículo 41 constitucional, pero sí adaptarlos al entorno digital.

A ello se suma la necesidad de regular con claridad la publicidad política digital. Debe exigirse la identificación verificable de anunciantes, un domicilio o una persona responsable en México, el monto gastado, el periodo de difusión, el alcance, las entidades en las que circuló el anuncio, la segmentación utilizada y su permanencia en repositorios públicos. Estos datos deben ser accesibles para autoridades, ciudadanía, periodistas, academia y partidos.

Otra necesidad pendiente es establecer obligaciones de etiquetado para el contenido generado o alterado con IA. Todo anuncio político, electoral o sobre temas sociales

que utilice IA debe advertirlo con claridad, para evitar que la ciudadanía sea confundida o manipulada con el uso de estas herramientas. Además, debe avanzarse hacia estándares técnicos de marcas de agua, metadatos o mecanismos de identificación interoperables entre plataformas.

Una propuesta adicional consiste en crear reglas específicas sobre microsegmentación electoral. Debe discutirse si ciertas prácticas deben limitarse o prohibirse durante campañas, en especial cuando se utilicen datos sensibles, perfiles emocionales o mensajes contradictorios dirigidos a distintos segmentos. La democracia requiere un espacio común de deliberación; en este sentido, la propaganda invisible y personalizada erosiona ese espacio.

Es clave también fortalecer la coordinación entre las plataformas y las autoridades electorales. La colaboración no debe depender solo de buena voluntad o memorándums. Deben existir canales institucionales claros, plazos de respuesta, protocolos de solicitud, mecanismos de emergencia, comunicación con OPLE y tribunales locales y criterios uniformes para atender violencia política, desinformación e interferencia electoral.

Otra ruta apunta a diseñar guías ciudadanas claras sobre IA y plataformas. La mesa identificó la necesidad de una guía comprensible para la sociedad civil. Esta guía debería explicar cómo identificar contenido manipulado, cómo reportarlo, cómo verificar información electoral, cómo entender por qué se ve un anuncio, cómo proteger cuentas personales y qué hacer ante violencia política digital. Esta propuesta se vincula con la materialización de la alfabetización digital, tema que fue abordado en otros seminarios.

A ello hay que sumar la necesidad de capacitar de manera directa a candidaturas y actores políticos. El diálogo destacó la importancia de jornadas de formación sobre buenas prácticas en contenido pagado, seguridad digital, autoprotección de mujeres en política, reporte de contenidos, transparencia publicitaria y prevención de suplantación de identidad. La capacitación no debe concentrarse solo en autoridades nacionales, sino llegar a ámbitos locales.

Urge ofrecer mejores respuestas institucionales ante la violencia política digital contra las mujeres y otros grupos de atención prioritaria. Deben existir mecanismos ágiles para retirar contenidos violentos, preservar evidencia, identificar patrones de sistematicidad y atender perfiles o páginas creadas para agredir. La respuesta institucional debe evitar dos extremos: dejar circular la violencia hasta que concluya un procedimiento largo o imponer a las víctimas cargas técnicas excesivas.

También debe avanzarse en la construcción de capacidades periciales digitales. Las autoridades electorales requieren herramientas para analizar *bots*, *astroturfing*,

deepfakes, patrones de difusión, bibliotecas de anuncios, metadatos, cuentas falsas, comportamiento inauténtico coordinado y financiamiento digital. La prueba técnica debe ayudar a investigar y resolver, no complicar de forma innecesaria los procedimientos.

Una distinción clave, que debe guiar cualquier legislación, decisión administrativa o criterio judicial, es la que existe entre los estándares de moderación privada y el sistema constitucional público de los países. Las plataformas pueden retirar o reducir la difusión de contenido conforme a sus políticas internas; por su parte, las autoridades estatales solo pueden sancionar con base en normas jurídicas. Por ello, México necesita tipos, infracciones, lineamientos y criterios suficientemente claros para evitar la arbitrariedad, garantizar la legalidad y permitir una actuación eficaz.

Es necesario revisar y reflexionar en torno a los modelos regulatorios de otros países, no con el propósito de trasplantarlos, sino de adaptarlos. Por ejemplo, la Unión Europea ofrece un modelo más robusto de regulación de plataformas, transparencia y servicios digitales; Brasil ha desarrollado mecanismos de intervención electoral frente a la desinformación. México debe estudiar sus efectos, aprender de sus aciertos y sus límites y construir un modelo propio.

Por último, es importante destacar que las intervenciones de la mesa de Ciudad de México tienen un hilo en común: la democracia digital exige pasar de la colaboración informal a la gobernanza democrática de las plataformas. Las redes sociales pueden ampliar la conversación pública, pero también pueden fragmentarla, manipularla o simularla. La justicia electoral cercana debe ser capaz de proteger la libertad de expresión sin entregar la integridad del debate público a reglas privadas opacas. Por ello, la preocupación que suscitan la IA y las plataformas digitales debe traducirse en una agenda regulatoria concreta. Esto implica actualizar el modelo de comunicación política, regular la publicidad digital, transparentar los anuncios, etiquetar contenidos generados con IA, limitar la microsegmentación dañina, fortalecer la cooperación con plataformas, además de capacitar a candidaturas, proteger a las mujeres en política, construir prueba técnica y formar una ciudadanía crítica. En la era algorítmica, la integridad electoral dependerá no solo de contar bien los votos, sino de cuidar las condiciones informativas en las que esos votos se deciden.



Análisis transversal



La revisión conjunta de los seis seminarios regionales permite advertir que la inteligencia artificial (IA), las plataformas digitales y la comunicación algorítmica ya forman parte del corazón de la vida electoral. El fenómeno no aparece como una amenaza futura ni como un tema periférico de innovación tecnológica. Se trata de una transformación que incide en la forma en que la ciudadanía recibe información, contrasta mensajes, construye preferencias, participa en campañas, denuncia irregularidades y confía o desconfía de los resultados. La disputa democrática se libra cada vez más en espacios diseñados por empresas privadas, ordenados por algoritmos, alimentados por datos y abiertos a formas inéditas de manipulación.

El recorrido territorial mostró que la justicia electoral mexicana enfrenta una tensión nueva: debe proteger libertades que han sido esenciales para la democracia, como la libertad de expresión, la crítica pública, el debate robusto y la creatividad política, pero también debe enfrentar usos de la tecnología que pueden erosionar las condiciones de una decisión libre, informada y con autenticidad. La IA puede servir para traducir información, facilitar el acceso a precedentes, apoyar la búsqueda de criterios, mejorar la comunicación institucional o hacer más accesibles los servicios públicos. Sin embargo, también puede crear imágenes, voces, vídeos y textos falsos verosímiles, segmentar mensajes según vulnerabilidades, amplificar ataques, ocultar financiamiento, dificultar la prueba y desplazar el debate público hacia circuitos opacos.

Los diálogos regionales contribuyeron a ordenar esta complejidad. Tijuana abrió la discusión desde la idea de democracia algorítmica y mostró que la equidad electoral debe pensarse también en términos de datos, plataformas y capacidad de segmentación. Arteaga profundizó en la dimensión probatoria y regulatoria, al colocar en el centro la trazabilidad, la autorregulación supervisada, la prueba técnica y la distinción entre uso legítimo y uso dañino. Morelia aportó una mirada ética y pedagógica, orientada a la autenticidad de la comunicación, al pensamiento crítico y a la necesidad de responder antes de que el daño

informativo se consume. Campeche introdujo una perspectiva de regulación comparada, estándares interamericanos, riesgos sistémicos, plataformas como intermediarias centrales de la conversación pública y la necesidad de adaptar modelos internacionales al contexto mexicano. Tlaxcala llevó el debate al campo de la argumentación jurídica, la prueba, las alucinaciones algorítmicas y la formación de operadores capaces de usar la tecnología sin quedar gobernados por ella. Ciudad de México cerró el recorrido con una discusión sobre gobernanza digital, colaboración con plataformas, moderación de contenidos, publicidad política y límites del modelo constitucional frente a actores privados globales.

El derecho debe actualizar sus categorías sin sacrificar garantías. La tecnología debe someterse a controles públicos sin quedar paralizada por el miedo. La democracia debe proteger la deliberación sin convertir la regulación en censura. En esa intersección se ubica la tarea de la justicia electoral cercana: una justicia que no puede limitarse a juzgar después de la jornada electoral, porque la manipulación de la voluntad ciudadana puede comenzar mucho antes, en la forma en que se produce, dirige, oculta y amplifica la información política.

Coincidencias regionales

La coincidencia más amplia entre las sedes fue reconocer que la democracia mexicana ya opera en un entorno algorítmico. Las redes sociales, los motores de recomendación, la publicidad digital, los datos personales, la IA generativa y las plataformas privadas forman parte del ecosistema ordinario de las campañas. La ciudadanía no recibe información política en un espacio neutral. La recibe en entornos que seleccionan, jerarquizan y amplifican contenidos con base en incentivos comerciales, patrones de atención, perfiles de consumo y estrategias de comunicación política. Esta realidad modifica el punto de partida de la justicia electoral, porque la integridad de una elección ya no depende solo de reglas sobre financiamiento, propaganda impresa, tiempos oficiales o *spots*. También depende de la integridad del espacio informativo previo al voto.

Todas las regiones coincidieron en que el marco jurídico mexicano todavía conserva una lógica construida para un mundo comunicativo cuya hegemonía es ya caduca. Las categorías tradicionales siguen siendo necesarias, pero resultan insuficientes frente a contenidos sintéticos, *deepfakes*, anuncios invisibles para el público general, mensajes enviados a segmentos específicos, *bots*, cuentas inauténticas, anonimato, manipulación

emocional y plataformas con reglas privadas de moderación. La libertad de expresión, la calumnia, la propaganda electoral, la violencia política, el interés superior de la niñez, la imparcialidad de las personas servidoras públicas y la equidad en la contienda deben dialogar ahora con nociones como trazabilidad, etiquetado, integridad informativa, seguridad digital, gobernanza de datos y responsabilidad algorítmica.

Otro punto de acuerdo fue que la IA no debe ser tratada como ilícita por sí misma. Su relevancia jurídica depende del uso, finalidad, contexto, transparencia, daño y grado de control humano. Puede servir para mejorar la justicia electoral, facilitar búsquedas de precedentes, traducir información, apoyar accesibilidad, ordenar expedientes, detectar patrones de desinformación o generar materiales para la ciudadanía. Pero puede ser usada también para suplantar identidades, fabricar noticias falsas, manipular audiencias, crear imágenes engañosas, amplificar la violencia política o distorsionar la voluntad del electorado. La agenda nacional no consiste en prohibir la tecnología, sino en distinguir sus usos legítimos de aquellos que dañan principios democráticos.

La tensión entre la libertad de expresión y la integridad electoral apareció en todas las sedes. La regulación de la comunicación digital debe cuidar que la sanción no inhiba la crítica, la sátira, el error genuino ni el debate intenso. Al mismo tiempo, la ausencia de reglas puede permitir que la libertad de expresión sea usada como cobertura para campañas de engaño, suplantación, propaganda encubierta o manipulación personalizada. La coincidencia regional fue clara: la respuesta no puede ser la censura preventiva generalizada ni la pasividad institucional.

Otro punto común fue la necesidad de impulsar una política pública de transparencia y etiquetado digital. En todas las sedes surgió la idea de que la ciudadanía tiene derecho a saber cuándo un contenido político fue generado o alterado con IA, quién lo produjo, quién lo pagó, en qué condiciones circuló y si fue dirigido a públicos específicos. El etiquetado no elimina el riesgo, pero permite que las personas evalúen el mensaje con información puntual. También ayuda a las autoridades a preservar evidencia, investigar responsabilidades y distinguir propaganda legítima de contenido diseñado para engañar. En la era digital, la transparencia ya no puede limitarse al monto del gasto reportado. Debe abarcar el origen del contenido, los criterios de difusión y la arquitectura de segmentación.

La microsegmentación fue una preocupación transversal en cada uno de los diálogos regionales. Las sedes coincidieron en que el acceso a datos y modelos de perfilamiento puede alterar la equidad en la contienda. Una campaña ya no necesita hablarle a todo el electorado con un mensaje común. Puede enviar mensajes distintos, incluso

contradictorios, a grupos definidos por edad, ubicación, creencias, consumo, emociones, miedos o historial digital. Esa comunicación fragmentada dificulta el escrutinio público, porque no todos pueden ver lo que se promete, se exagera o se manipula ante cada audiencia. La deliberación democrática pierde un espacio común y se convierte en una suma de conversaciones cerradas.

La dificultad probatoria también apareció en la serie de diálogos. Para sancionar un contenido sintético o una campaña de desinformación, la autoridad debe saber si el contenido fue generado con IA y, además, definir quién lo produjo, quién lo difundió, quién lo financió, qué alcance tuvo, a quién benefició y si existió coordinación. Esa tarea exige peritajes, análisis de metadatos, preservación de evidencia, trazabilidad de la pauta, revisión de patrones de circulación y comprensión de modelos generativos. El problema se agrava porque los tiempos electorales son breves. Cuando la investigación tarda, el daño comunicativo puede haberse producido y la decisión puede llegar tarde para reparar la afectación.

Otra coincidencia medular fue que las plataformas privadas ocupan un lugar central en la conversación pública. Aunque no son autoridades electorales, sus reglas de moderación, sus sistemas de anuncios, sus algoritmos y sus decisiones de retiro o permanencia de contenidos inciden en la competencia democrática. Las sedes mostraron la necesidad de colaboración con las plataformas, pero también la insuficiencia de una relación fundada solo en la buena voluntad. La agenda nacional exige canales claros de comunicación, tiempos de respuesta, preservación de evidencia, transparencia en la publicidad política, atención a las órdenes electorales y criterios de responsabilidad cuando exista tolerancia o facilitación de prácticas dañinas.

La relación entre IA y la función jurisdiccional fue otro consenso relevante. El Tribunal Electoral del Poder Judicial de la Federación y las autoridades electorales pueden aprovechar herramientas algorítmicas para mejorar búsquedas, organizar información, apoyar el análisis de precedentes y hacer más accesible la justicia. Sin embargo, todos los diálogos subrayaron que la IA debe ser una herramienta de apoyo y no un sustituto del juicio jurídico. La decisión jurisdiccional exige responsabilidad humana, valoración contextual, argumentación, ponderación de derechos y control ético. Las herramientas pueden alucinar, replicar sesgos, inventar datos o producir respuestas con apariencia de certeza. Por ello, su uso interno requiere supervisión, auditoría, protección de datos y trazabilidad.

La educación cívica digital cerró el conjunto de coincidencias, pues se reconoció que la manipulación electoral no se combate solo con sanciones, sino que requiere una

ciudadanía capaz de reconocer *deepfakes*, publicidad segmentada, cuentas falsas, cadenas fabricadas, mensajes emocionales, *bots*, cámaras de eco y propaganda encubierta. Las sedes insistieron en que la integridad electoral del siglo XXI exige alfabetización digital, pensamiento crítico y formación interdisciplinaria. La justicia electoral cercana debe ser también una justicia pedagógica, capaz de explicar riesgos y fortalecer capacidades ciudadanas.

Prioridades regionales

Las coincidencias nacionales no eliminan, por supuesto, las diferencias regionales. El valor del recorrido está, en buena medida, en mostrar que la transformación digital de la democracia no se vive del mismo modo en todos los territorios ni se piensa desde las mismas preocupaciones. Cada sede aportó una mirada distinta al problema y, de esta manera, mostró la necesidad de soluciones flexibles, con estándares comunes y sensibilidad contextual.

Tijuana colocó la discusión desde una región fronteriza, tecnológica y conectada con flujos intensos de información. Su aporte consistió en abrir el tema desde la noción de democracia algorítmica. Allí se insistió en que la equidad electoral ya no puede analizarse solo a partir del dinero o del acceso a medios tradicionales. Los datos, la segmentación, la huella digital y la capacidad de personalizar mensajes se convirtieron en factores de poder electoral. También se sostuvo que la IA puede apoyar la labor jurisdiccional, pero exige controles sobre la calidad de los datos, la seguridad de la información y la supervisión humana. Tijuana permitió mirar el fenómeno desde su dimensión estructural. La democracia ya está atravesada por algoritmos y el derecho debe reconocerlo.

Arteaga, por su parte, aportó una mirada técnica, probatoria y constitucional. Al desarrollarse en una institución especializada en derechos humanos, el debate se concentró en cómo armonizar la innovación, la libertad de expresión, la protección de datos, el derecho a la información, la equidad y la imparcialidad. La sede profundizó en la idea de la IA como medio comisivo y no como conducta ilícita por sí misma. También ofreció una aproximación fina a la trazabilidad del contenido, los metadatos, la perplejidad, las alucinaciones algorítmicas y la necesidad de peritajes especializados. Su contribución fue advertir que la justicia electoral del futuro no requerirá solo argumentos jurídicos sólidos; también necesitará capacidades técnicas para detectar, probar y frenar manipulaciones digitales.

Morelia llevó el debate hacia una dimensión ética, comunicativa y pedagógica. En esa sede se subrayó la brecha entre la velocidad del cambio tecnológico y la lentitud del derecho. También se insistió en que la IA altera la percepción de la realidad y que la ciudadanía puede recibir contenidos con apariencia auténtica sin saber si fueron producidos por una persona o por una máquina. Morelia colocó el pensamiento crítico como condición democrática y sostuvo que la integridad electoral no se limita a contar bien los votos. También exige proteger el entorno informativo que permite formar la voluntad ciudadana. Su aporte fue recordar que la tecnología no sustituye la responsabilidad democrática, sino que la hace más urgente.

Campeche ofreció una perspectiva vinculada con la regulación comparada, los estándares internacionales y los riesgos sistémicos. Desde esta sede se discutió la necesidad de no importar modelos externos sin adaptación, pero sí aprender de experiencias que han intentado regular IA, propaganda digital, riesgos de plataformas y transparencia publicitaria. En esta sede cobraron importancia los modelos de gobernanza, la noción de plataformas como intermediarias centrales del flujo informativo, la protección interamericana de la libertad de expresión y el riesgo de que la regulación se convierta en censura si no se diseña con cuidado. Campeche aportó una mirada de adaptación institucional, al preguntar cómo convertir principios técnicos y comparados en reglas comprensibles para autoridades, ciudadanía y actores políticos.

Tlaxcala introdujo una discusión de mayor densidad metodológica. La sede no se concentró solo en propaganda digital o plataformas, sino en la relación entre IA y razonamiento jurídico. Allí se discutió cómo la IA interviene en la investigación, la redacción de demandas, la elaboración de sentencias y la argumentación. La preocupación fue que el derecho no puede adoptar herramientas algorítmicas sin método. La teoría de la argumentación, la ética profesional, la teoría de la prueba y el control inferencial deben orientar su uso. Tlaxcala también insistió en que la ciudadanía crítica y la formación de operadores jurídicos son condiciones para gobernar la tecnología sin quedar sometidos a ella.

Ciudad de México cerró el recorrido con una mirada de gobernanza digital desde el centro institucional del país. La región permitió discutir el papel de las plataformas globales, las políticas de moderación, las bibliotecas de anuncios, las etiquetas de contenido sintético, las redes inauténticas, la colaboración con autoridades, la violencia política digital y los límites del modelo mexicano frente a empresas privadas con poder transnacional. La presencia de una representante de una plataforma permitió observar las tensiones entre autorregulación, deberes de transparencia, moderación privada

y control público. La sede metropolitana aportó una lectura institucional madura. La justicia electoral no puede resolver sola el problema. Necesita gobernanza compartida, pero bajo reglas democráticas.

Estas diferencias territoriales muestran que la agenda no puede reducirse a una sola respuesta. Por tanto, la lectura nacional debe integrar estos enfoques sin borrar sus matices. La justicia electoral cercana debe aprender de cada región porque cada una ilumina una parte distinta del mismo fenómeno.

Problemas emergentes

Los diálogos permitieron identificar cuestiones que no estaban previstas con la misma intensidad al inicio del proyecto o que adquirieron mayor relevancia a partir del intercambio territorial.

Una de ellas fue la noción de autenticidad como bien democrático. La discusión sobre IA no se limita a la verdad o falsedad de un contenido. También involucra la posibilidad de que la ciudadanía sepa si aquello que ve, escucha o lee corresponde a una persona real, a un hecho verificable, a una opinión humana, a una edición legítima o a un contenido fabricado. En la era de los contenidos sintéticos, la autenticidad de la comunicación se vuelve parte de la integridad electoral.

Emergió también la idea de autoridad sintética en la conversación pública. La IA puede crear voces, rostros y mensajes que aparentan respaldo ciudadano, testimonio social o liderazgo político. Aunque no exista una persona real detrás de una imagen, el contenido puede generar efectos emocionales y políticos. Este problema apareció con fuerza en los casos de imágenes de niñas, niños o adolescentes creadas con IA, pero se extiende a otros supuestos. La propaganda puede simular apoyo social, victimización, indignación o cercanía a grupos vulnerables mediante personajes inexistentes. La justicia electoral deberá preguntarse qué protege cuando el contenido no lesiona a una persona concreta, pero sí afecta la deliberación pública.

Las autoridades electorales, sin embargo, no solo necesitan nuevas reglas sustantivas; requieren también de capacidad para conservar, analizar y valorar evidencia que cambia, desaparece o se replica con rapidez. Una publicación puede borrarse; un anuncio puede haber sido visible solo para un segmento de personas usuarias; un contenido puede circular en mensajería privada; un video puede ser alterado con herramientas accesibles; una red de *bots* puede operar desde varios

países. Esta realidad exige protocolos de preservación, peritajes ágiles y criterios de valoración que no dependan solo de capturas de pantalla o impresiones visuales.

La moderación privada de contenidos también se incorporó como parte de una agenda emergente. Las plataformas toman decisiones que afectan el debate electoral. Pueden retirar publicaciones, suspender cuentas, etiquetar contenido, reducir alcance, bloquear anuncios o permitir que ciertas campañas continúen. Estas decisiones tienen impacto público, aunque provengan de empresas privadas. El problema es que la moderación puede proteger derechos o convertirse en censura. La justicia electoral tendrá que construir criterios para relacionarse con las plataformas sin sustituirlas, pero sin aceptar que sus reglas privadas definan por sí solas las condiciones de la conversación democrática.

La seguridad tecnológica de los procesos electorales también adquirió relevancia. La discusión no se limitó a la propaganda digital. También se habló de ciberseguridad, sistemas de información, protección de datos, herramientas internas de tribunales, integridad de expedientes, uso de IA en tareas jurisdiccionales y riesgo de dependencia tecnológica. La integridad electoral del siglo XXI exige proteger infraestructuras, no solo discursos. Los ataques informáticos, las filtraciones, la manipulación de bases de datos o la vulnerabilidad de sistemas pueden afectar la confianza pública incluso si no alteran los resultados.

Otro problema emergente fue el uso de IA por las propias autoridades. La IA puede mejorar servicios, pero también plantea riesgos de sesgo, error, opacidad, automatización indebida y pérdida de responsabilidad. Herramientas como buscadores de precedentes, sistemas de apoyo a la redacción, análisis de expedientes o modelos de clasificación deben operar bajo principios de supervisión humana, seguridad, auditabilidad y protección de datos. La autoridad electoral no puede exigir transparencia a actores externos y, al mismo tiempo, usar sistemas opacos en su propia labor.

Por último, surgió una preocupación por la erosión de la confianza; es decir, la proliferación de contenidos sintéticos puede producir no solo engaños concretos, sino un efecto más profundo. Si todo puede ser falso, la ciudadanía puede dejar de creer incluso en información verdadera. Este fenómeno amenaza la base misma de la deliberación. La justicia electoral deberá proteger no solo casos individuales, sino el ecosistema de confianza que permite que una elección sea aceptada como legítima.

Vacíos normativos o interpretativos

El vacío más evidente es la ausencia de un marco electoral específico sobre IA, plataformas digitales y propaganda algorítmica. México cuenta con principios constitucionales y normas generales que pueden aplicarse a ciertos casos, pero carece de una arquitectura integral que regule contenidos sintéticos, etiquetado, microsegmentación, publicidad digital, *bots*, *deepfakes*, responsabilidad de plataformas, trazabilidad de anuncios, uso de datos personales y estándares de prueba. Esta ausencia obliga a resolver caso por caso, con categorías que no siempre fueron diseñadas para el entorno digital.

Existe, a su vez, un vacío en materia de etiquetado y transparencia de contenidos generados o alterados con IA. La ciudadanía necesita saber cuándo está frente a un audio, un video, una imagen o un texto sintético. Sin esa advertencia, el contenido puede producir efectos de engaño aun cuando no contenga una falsedad verificable. La regulación debe definir cuándo procede el etiquetado, quién debe colocarlo, qué contenido debe cubrir, cómo se conserva la evidencia y qué consecuencias surgen ante el incumplimiento. El estándar debe cuidar que la obligación no se convierta en censura ni en una carga imposible para expresiones ciudadanas de bajo impacto.

La microsegmentación política requiere un desarrollo normativo propio. Deben definirse límites al uso de datos personales, información sensible, perfiles psicológicos, vulnerabilidades emocionales, ubicación, historial de consumo y patrones de interacción. También se requiere un archivo público de anuncios políticos que permita conocer mensajes, públicos objetivo, montos, responsables y criterios de segmentación. La propaganda electoral no puede quedar oculta en circuitos cerrados en los que solo la ve la audiencia elegida por la campaña.

La fiscalización de la pauta digital presenta vacíos relevantes, pues, si bien las reglas tradicionales permiten rastrear ciertos gastos visibles, no siempre captan anuncios segmentados, contenidos orgánicos pagados de modo indirecto, *influencers*, proveedores de datos, agencias de análisis, redes de amplificación, pauta en plataformas extranjeras o campañas coordinadas sin reporte. La justicia electoral y las autoridades administrativas necesitan criterios para identificar el gasto, el beneficio, la coordinación y la responsabilidad. Sin esa actualización, la equidad puede erosionarse por vías no registradas.

Falta, además, un estándar claro sobre responsabilidad en cadenas digitales. Debe distinguirse entre la persona que crea contenido y quien lo financia, quien lo pauta, quien lo amplifica, quien lo aloja, quien se beneficia y quien tiene capacidad de

retirarlo. Las plataformas no pueden ser responsables por todo lo que ocurre en sus sistemas, pero tampoco pueden considerarse ajenas cuando administran publicidad política, sistemas de recomendación y reglas de moderación. Los partidos y las candidaturas no pueden eludir responsabilidad cuando se benefician de campañas coordinadas o financiamiento opaco. La imputación debe ser precisa y basada en el conocimiento, el control, el beneficio, la coordinación y la capacidad de prevención.

La prueba de IA y desinformación es otro ámbito sin criterios consolidados. Se necesitan reglas sobre metadatos, peritajes, preservación de evidencia, análisis de redes, indicadores de generación sintética, autenticidad de archivos, cadena de custodia digital, alcance del contenido y valoración del impacto. También se requiere definir qué grado de certeza es necesario para dictar medidas cautelares, ordenar el etiquetado, retirar contenido o imponer sanciones. La respuesta debe ser rápida, pero no arbitraria.

La regulación de *deepfakes* y de la suplantación de identidad también requiere mayor precisión. La voz, la imagen, el rostro, los gestos y el estilo de una persona pueden ser imitados con herramientas de bajo costo. En campañas, ello puede afectar el honor, la reputación, la libertad de expresión, la equidad y el derecho a la información. Deben existir protocolos de reacción rápida, pero con garantías. La autoridad debe distinguir entre la parodia, la sátira, la crítica, la edición evidente y la suplantación engañosa con capacidad de daño electoral.

La relación con las plataformas digitales carece de reglas con suficiente fuerza. Se necesitan obligaciones de respuesta, representación jurídica, preservación de evidencia, transparencia de la publicidad política, reportes sobre redes inauténticas, criterios de moderación y canales para atender medidas cautelares. La colaboración voluntaria puede ayudar, pero no sustituye un marco de responsabilidades democráticas. La conversación electoral no puede depender solo de reglas privadas.

Otra omisión significativa tiene que ver con el uso interno de IA en las autoridades electorales y jurisdiccionales. Deben definirse principios de gobernanza, auditoría, seguridad, protección de datos, explicabilidad, supervisión humana, prohibición de automatizar decisiones sustantivas y trazabilidad de usos. Las herramientas de apoyo pueden ser valiosas, pero deben operar bajo reglas institucionales claras. La confianza en la justicia electoral exige saber que la decisión sigue siendo humana, razonada y revisable.

La ciberseguridad electoral requiere un tratamiento más visible. Los principios clásicos de certeza, legalidad, independencia, imparcialidad, objetividad y máxima publicidad deben dialogar con la integridad tecnológica, la protección de datos, la

resiliencia de los sistemas y la prevención de ataques. Este punto incluye plataformas de denuncia, sistemas de expedientes, bases de datos, cómputos, comunicación institucional, páginas de autoridades y herramientas de difusión pública. La seguridad digital no es solo un asunto técnico; es condición de confianza democrática.

Falta también una política pública de alfabetización cívica digital con anclaje electoral. La educación no debe dejarse a campañas ocasionales. Debe formar parte de una estrategia sostenida que involucre a autoridades electorales, escuelas, universidades, medios, plataformas y sociedad civil. La ciudadanía debe aprender a reconocer la manipulación, verificar fuentes, entender la publicidad segmentada, identificar contenidos sintéticos y denunciar irregularidades. Sin una ciudadanía crítica, la regulación llegará tarde.

Al cierre, los vacíos interpretativos muestran que la justicia electoral debe construir una doctrina sobre integridad informativa. Esa doctrina tendría que proteger la libertad de expresión y, al mismo tiempo, reconocer que la autonomía del voto se debilita cuando la ciudadanía recibe información fabricada, dirigida en secreto o amplificada mediante redes opacas. La integridad electoral ya no puede verse solo como la regularidad de la jornada o la exactitud del cómputo. Debe incluir las condiciones informativas que permiten que la voluntad ciudadana se forme con libertad.

La lectura nacional que surge de los diálogos es clara. La IA y las plataformas digitales no deben ser vistas como cuerpos extraños frente a la democracia electoral. Ya forman parte de ella. El reto consiste en gobernarlas sin sofocar la libertad, aprovecharlas sin entregarles la decisión pública y regular sus usos dañinos sin paralizar la innovación. En ese equilibrio se jugará buena parte de la confianza democrática en los próximos procesos electorales. La justicia electoral cercana deberá ser, en esta materia, una justicia con capacidad técnica, sensibilidad constitucional, vocación pedagógica y compromiso con una deliberación pública libre de manipulación.



Agenda para la justicia electoral



El recorrido regional y el análisis transversal permiten proyectar este volumen hacia una agenda de futuro para la justicia electoral mexicana. La inteligencia artificial (IA) y las plataformas digitales ya no pueden ser tratadas como un fenómeno externo al derecho electoral ni considerarse cuestiones reservadas a especialistas técnicos. Hoy forman parte de las condiciones bajo las cuales se informa la ciudadanía, se construyen preferencias políticas, se despliegan campañas, se amplifican discursos, se produce prueba y se disputan los sentidos de la democracia.

La pregunta central, entonces, ya no es si la tecnología debe entrar o no al campo electoral. Esa pregunta quedó superada por la realidad. Los actores políticos usan herramientas de generación de contenido, publicidad digital, datos personales, segmentación, redes de difusión, *bots*, mensajes personalizados y estrategias de amplificación. Las plataformas privadas organizan buena parte de la conversación pública. Las autoridades electorales utilizan sistemas de información, buscadores, expedientes digitales y herramientas de apoyo. La ciudadanía recibe contenidos que muchas veces no sabe si fueron escritos, editados, generados o distribuidos por personas, por máquinas, por campañas o por redes coordinadas.

La agenda para la justicia electoral debe partir de esa nueva condición democrática. La integridad de una elección no depende solo de la jornada, del cómputo o de la fiscalización de gastos visibles. También depende de la calidad del entorno informativo previo al voto. Una elección puede tener boletas correctas, casillas instaladas y resultados verificables, pero aun así enfrentar un deterioro profundo si la ciudadanía decide a partir de engaños, contenidos sintéticos no identificados, campañas de miedo, manipulación por datos, suplantaciones de identidad, violencia digital o publicidad oculta.

Esto no significa que la respuesta deba ser prohibir la IA o cerrar el espacio digital. Una democracia constitucional debe proteger la libertad de expresión, la crítica y el debate intenso. También debe reconocer que la tecnología puede mejorar la justicia

electoral, hacer más accesibles los criterios, traducir información, facilitar búsquedas, apoyar la sistematización de precedentes y acercar a la ciudadanía a instituciones complejas. El reto consiste en distinguir entre el uso legítimo y el uso dañino, es decir, entre innovación y manipulación, entre creatividad política y engaño, entre segmentación informativa y explotación de vulnerabilidades, etcétera.

En este contexto, el Tribunal Electoral del Poder Judicial de la Federación (TEPJF) no solo tendrá que resolver casos sobre imágenes generadas con IA, *deepfakes*, propaganda digital, *bots*, violencia política digital, calumnia o publicidad segmentada. Sobre todo, deberá construir una doctrina constitucional sobre integridad informativa, autenticidad del debate público, responsabilidad digital, trazabilidad de contenidos y protección de la autonomía del voto. Esa doctrina deberá ser técnica sin perder sensibilidad democrática.

Retos jurisdiccionales

La justicia electoral enfrenta un reto muy particular desde el momento en que el uso de la IA empezó a adquirir relevancia jurídica. La tecnología no debe ser sancionada por su mera existencia. Lo relevante, entonces, es el uso que se le da, el contexto electoral en el que opera, si hay engaño, intención de manipular, menoscabo en derechos, ventaja indebida en la competencia y desinformación que afecta el ejercicio de un voto libre.

La IA deberá ser entendida como un posible medio de comisión, no como infracción autónoma en todos los casos. Este punto será clave para evitar respuestas excesivas o insuficientes. Un contenido generado con IA puede ser legítimo si informa, traduce, hace accesible un mensaje, explica una propuesta o facilita la comunicación ciudadana. Pero puede ser ilícito si oculta su origen sintético o si suplanta la voz o la imagen de una persona, fabrica hechos, distorsiona declaraciones, genera propaganda encubierta, reproduce violencia política digital o dirige mensajes manipuladores a grupos vulnerables. La jurisdicción deberá construir criterios capaces de distinguir estos supuestos sin convertir la regulación en censura.

El derecho electoral tendrá que decidir cómo valorar audios, videos, imágenes y textos cuya apariencia ya no basta para acreditar su origen. La pregunta no será solo qué dice un contenido, sino cómo se produjo, quién lo financió, quién lo difundió, si fue editado, si fue generado por una herramienta algorítmica, si se presentó como real y si la ciudadanía tuvo elementos para advertir su naturaleza. La autenticidad se convertirá en una condición de la integridad electoral.

Los *deepfakes* y la suplantación de identidad plantearán controversias de alto impacto. Una candidatura puede aparecer en un video diciendo algo que nunca dijo; una persona servidora pública puede ser simulada en un audio; una mujer candidata puede ser atacada mediante contenido sexualizado o degradante generado con IA. La justicia electoral deberá proteger el honor, la imagen, la dignidad, la libertad de expresión, la equidad y el derecho a la información, sin perder de vista que no toda edición, sátira o parodia debe recibir el mismo tratamiento.

También llegarán más casos sobre niñas, niños y adolescentes representados mediante imágenes sintéticas. Los precedentes iniciales mostraron un problema complejo. Si la imagen no corresponde a una persona menor de edad real, quizá no exista afectación directa al derecho a la imagen de una niña o niño concreto. Sin embargo, el contenido puede producir efectos propagandísticos, emocionales o de manipulación. Puede instrumentalizar la figura infantil para generar empatía, miedo, indignación o respaldo político. La jurisdicción deberá analizar no solo la existencia de una persona real, sino también el efecto comunicativo, la finalidad electoral y la obligación de advertir que se trata de contenido generado con IA.

El TEPJF también tendrá que revisar si ciertos mensajes personalizados afectan la equidad, el derecho a la información o la libertad del voto. La dificultad reside en que la propaganda microsegmentada no siempre es visible para todos. Puede dirigirse solo a jóvenes, mujeres, personas mayores, grupos religiosos, regiones específicas, personas indecisas o perfiles construidos con datos de consumo. Si cada grupo recibe un mensaje distinto, el debate público pierde un espacio común de contraste. La justicia electoral deberá definir cuándo la segmentación es una herramienta legítima de comunicación y cuándo se convierte en manipulación opaca.

Por otro lado, los procedimientos electorales exigen rapidez, pero los conflictos digitales demandan análisis técnico. Para acreditar que un contenido fue generado con IA puede ser necesario revisar metadatos, patrones lingüísticos, origen de archivos, trazabilidad de la difusión, redes de amplificación, pauta digital, cuentas coordinadas, peritajes audiovisuales o registros de plataformas. La jurisdicción deberá construir estándares probatorios que permitan actuar con oportunidad sin resolver a partir de intuiciones. En las medidas cautelares, el umbral no podrá ser idéntico al de una sentencia de fondo, pero tampoco puede descansar en sospechas sin soporte.

Si se considera que, en el entorno digital, el daño puede surgir de una cadena compleja de conductas y acciones, entonces, será necesario definir criterios de imputación y de responsabilidad. Basta pensar en un ejemplo: una persona crea el contenido, otra

lo paga, una agencia lo pauta, una red social lo amplifica y distribuye y una candidatura se beneficia de este impacto en la esfera pública. La pregunta jurisdiccional será a quién atribuir responsabilidad, con qué estándar de conocimiento, qué grado de control se exige, cómo probar la coordinación y cuándo puede presumirse un beneficio electoral. Sin reglas de imputación, las infracciones digitales pueden quedar impunes o sancionarse de forma injusta.

Las redes sociales, como se sabe, pueden amplificar ataques contra mujeres, personas de la diversidad sexual, comunidades, candidaturas y personas servidoras públicas. La IA puede intensificar ese daño mediante contenidos sintéticos, memes degradantes, voces falsas, imágenes sexualizadas o campañas anónimas. La justicia electoral tendrá que proteger a las víctimas sin inhibir el debate público. También deberá actuar con rapidez, porque en el entorno digital el daño se produce antes de que las resoluciones lleguen.

Asimismo, el uso interno de IA en la función jurisdiccional planteará retos propios. Las herramientas de apoyo pueden facilitar la búsqueda de precedentes, la organización de información, la traducción, la clasificación de expedientes y la elaboración de materiales ciudadanos. Pero la decisión jurisdiccional debe seguir siendo humana, razonada y responsable. El TEPJF deberá definir protocolos de uso, auditoría, supervisión, protección de datos, verificación de resultados y límites frente a tareas sustantivas. Una justicia electoral que exige transparencia a campañas y plataformas debe aplicar también criterios de transparencia a sus propias herramientas.

Retos institucionales

La agenda institucional exige reconocer que ningún actor puede enfrentar solo los desafíos digitales de la democracia. El TEPJF, el Instituto Nacional Electoral (INE), los organismos públicos locales electorales (OPLE), los tribunales locales, las fiscalías electorales, las plataformas, las universidades, los partidos políticos, las organizaciones civiles, las empresas de verificación, los centros de investigación y la ciudadanía forman parte de un ecosistema que requiere coordinación. La manipulación digital cruza competencias, fronteras y tiempos procesales. Por ello, la respuesta debe ser interinstitucional, técnica y sujeta a reglas claras.

Un reto central, en este contexto, será construir capacidades especializadas dentro de las autoridades electorales y jurisdiccionales. Resolver controversias digitales exige

comprender cómo funcionan la pauta, los algoritmos de recomendación, los *bots*, los metadatos, los contenidos sintéticos, la viralización, la segmentación, las bibliotecas de anuncios y las redes de amplificación. No basta con trasladar categorías del mundo analógico. La justicia electoral necesita equipos técnicos, peritajes ágiles, laboratorios de análisis digital, protocolos de preservación de evidencia y formación continua para personas juzgadoras y funcionariado.

También será indispensable crear un lenguaje común entre el derecho, la tecnología y la democracia. Las autoridades electorales pueden conocer principios constitucionales, pero no siempre dominan la arquitectura técnica de las plataformas. Las plataformas pueden comprender sus sistemas, pero no siempre entienden las exigencias del proceso electoral mexicano. La ciudadanía usa redes y herramientas de IA sin conocer sus mecanismos de recomendación, perfilamiento o monetización. Si cada actor habla desde un lenguaje distinto, la coordinación será frágil. La formación interdisciplinaria debe convertirse en política institucional.

La colaboración con las plataformas digitales será uno de los puntos más sensibles. Las plataformas no son autoridades electorales, pero sus decisiones inciden en el debate público. Pueden retirar contenido, suspender cuentas, etiquetar publicaciones, limitar alcance, archivar anuncios o preservar evidencia. Esta colaboración no debe depender solo de acuerdos informales o de la buena voluntad empresarial. Se requieren canales de contacto, plazos de respuesta, representación jurídica, protocolos de cumplimiento, transparencia sobre publicidad política y mecanismos para atender medidas cautelares. La moderación privada no puede sustituir al control constitucional, pero tampoco puede quedar fuera de la gobernanza electoral.

La coordinación entre autoridades administrativas y jurisdiccionales también deberá fortalecerse. El INE y los OPLE tienen capacidades de fiscalización, monitoreo, capacitación y organización. Los tribunales resuelven controversias y definen criterios. Las fiscalías pueden investigar conductas graves. Si cada institución actúa por separado, la respuesta llegará tarde o será incompleta. Los casos de desinformación coordinada, pauta oculta o suplantación de identidad requieren preservación inmediata de evidencia, medidas preventivas, análisis técnico y resolución con garantías. La coordinación debe planearse antes del proceso electoral, no durante la crisis.

La creación de sistemas de monitoreo electoral digital aparece como una línea institucional necesaria. No se trata de vigilar toda la conversación ciudadana ni de construir un mecanismo de censura. Se trata de identificar patrones públicos de desinformación, redes coordinadas, *deepfakes*, suplantaciones, publicidad política no reportada,

violencia digital y riesgos para la integridad electoral. Un modelo de monitoreo con participación de autoridades, universidades y especialistas puede generar alertas, preservar evidencia y apoyar decisiones sin sustituir la investigación formal ni limitar la expresión ciudadana.

La ciberseguridad deberá ocupar un lugar central si se considera que la integridad electoral no depende solo de contenidos. En efecto, también depende de sistemas, bases de datos, plataformas de denuncia, herramientas de consulta, expedientes digitales, sitios institucionales, mecanismos de cómputo, redes internas y canales de comunicación. Un ataque informático, una filtración o una caída de sistemas puede afectar la confianza pública, aunque no altere resultados. La justicia electoral del futuro deberá asumir que la certeza electoral también requiere resiliencia tecnológica.

Las instituciones deberán definir, a partir de lineamientos y protocolos, los usos que le den a la IA para sus tareas internas. El uso de buscadores, asistentes de redacción, clasificadores de información, herramientas de traducción o sistemas de apoyo debe sujetarse a reglas. Debe saberse qué datos se usan, qué tareas se automatizan, qué supervisión existe, qué riesgos de sesgo o error se han identificado y qué decisiones quedan fuera de cualquier automatización. La innovación institucional será legítima si se acompaña de gobernanza, auditoría y responsabilidad.

Las autoridades electorales han desarrollado durante décadas estrategias de educación sobre el voto, las instituciones y la participación. Ahora deben incorporar contenidos sobre *deepfakes*, publicidad segmentada, *bots*, cadenas falsas, cuentas inauténticas, verificación de fuentes, protección de datos y manipulación emocional. Esta tarea debe involucrar a escuelas, universidades, medios públicos, plataformas y organizaciones sociales. La ciudadanía no puede defender su voto si no entiende el entorno informativo en el que se forma.

Los partidos políticos y las candidaturas deberán asumir deberes institucionales más estrictos. No pueden presentarse solo como personas usuarias de plataformas; son actores con responsabilidad democrática. Deben evitar el uso de contenidos sintéticos engañosos, transparentar pauta digital, abstenerse de campañas coordinadas opacas, no explotar datos sensibles y capacitar a sus equipos en ética digital. La competencia electoral no puede convertirse en una carrera por manipular mejor al electorado.

Retos normativos

La agenda normativa debe partir de una premisa básica: México requiere un marco específico sobre IA, plataformas digitales y elecciones, pero ese marco no debe ser rígido ni adverso a la tecnología. Una regulación cerrada puede quedar obsoleta en poco tiempo; una regulación ausente deja a las autoridades y a la ciudadanía sin herramientas. El diseño debe combinar principios constitucionales, obligaciones mínimas, estándares técnicos actualizables, lineamientos flexibles, cooperación institucional y control judicial.

El primer campo de desarrollo normativo será el etiquetado de contenidos generados o alterados con IA. La ley o los lineamientos deben definir cuándo un contenido político debe identificarse como sintético, qué grado de alteración activa esa obligación, quién debe colocar la advertencia, cómo debe ser visible, qué ocurre cuando se omite y qué autoridad puede ordenar correcciones. La obligación debe concentrarse en propaganda electoral, mensajes de partidos, candidaturas, personas servidoras públicas, campañas pagadas y contenidos con capacidad de incidir en derechos o en la competencia. No debe convertirse en carga desproporcionada para expresiones ciudadanas de bajo impacto.

La regulación de *deepfakes* deberá recibir un tratamiento propio. Los contenidos que simulan la voz, el rostro, los gestos, las declaraciones o los actos de una persona requieren protocolos de reacción rápida. El marco normativo debe distinguir la parodia, la sátira, la edición evidente, la recreación artística y la suplantación engañosa. También debe prever medidas cautelares, preservación de evidencia, rectificación, etiquetado, retiro proporcional y sanciones cuando exista dolo, daño a derechos, afectación de la equidad o riesgo de manipulación del voto.

Debe regularse el uso de datos personales, información sensible, perfiles psicológicos, ubicación, religión, edad, consumo, intereses y vulnerabilidades emocionales. La publicidad política segmentada no debería operar sin trazabilidad. La ciudadanía tiene derecho a conocer qué anuncios circulan, quién los paga, a quién se dirigen, qué criterios de segmentación se usan y cuánto se invierte. Un archivo público de anuncios políticos ayudaría a reconstruir el debate, facilitar la fiscalización y evitar campañas invisibles.

La publicidad digital y el financiamiento de campañas requieren reglas de fiscalización actualizadas. La legislación debe cubrir anuncios en plataformas, contratación de *influencers*, agencias de datos, proveedores de IA, sistemas de automatización, redes

de cuentas, contenidos orgánicos pagados, servicios extranjeros y campañas de amplificación. El gasto digital no puede quedar sin reportarse por su complejidad técnica. También debe analizarse el beneficio electoral cuando la pauta se realiza por terceros, simpatizantes o estructuras coordinadas.

La responsabilidad de las plataformas digitales deberá definirse con cuidado. Las plataformas no pueden responder por cada expresión ciudadana publicada en sus sistemas. Pero sí tienen deberes cuando administran publicidad política, monetizan contenidos, tienen conocimiento de campañas coordinadas, reciben órdenes de autoridad, conservan evidencia o permiten suplantaciones que impliquen riesgo electoral. El marco normativo debe establecer obligaciones de transparencia, canales de respuesta, reportes públicos, preservación de evidencia, cooperación con las autoridades y revisión de decisiones de moderación. La democracia no puede depender solo de reglas privadas de empresas globales.

Debe considerarse, a su vez, una regulación sobre *bots*, cuentas inauténticas y redes coordinadas. No toda automatización es dañina. Puede usarse para atención ciudadana, difusión institucional o accesibilidad. El problema surge cuando se simula apoyo social, se amplifica desinformación, se ataca a candidaturas, se manipulan tendencias o se oculta la fuente de la propaganda. La norma debe distinguir la automatización legítima de una operación encubierta y prever consecuencias frente a campañas coordinadas con finalidad electoral.

Otro frente regulatorio es la integración de la protección de datos personales al derecho electoral digital. La microsegmentación política descansa en datos. Muchos de ellos pueden revelar preferencias, salud, religión, ubicación, edad, hábitos, redes de contacto o rasgos sensibles. La regulación electoral debe dialogar con el régimen de protección de datos para impedir que la persuasión política se construya mediante la explotación opaca de información personal. La autonomía del voto exige que los datos no se usen como herramienta de manipulación.

Los lineamientos sobre niñas, niños y adolescentes deberán actualizarse frente a contenidos sintéticos. El análisis no puede quedar limitado al consentimiento o al derecho de imagen de personas reales. Deben considerarse efectos comunicativos, instrumentalización emocional, apariencia de realidad, contexto electoral y advertencias al público. La figura infantil, aun generada por IA, puede ser usada para producir empatía, miedo o indignación con fines de propaganda.

Deben establecerse criterios sobre capturas, enlaces, descargas, metadatos, cadena de custodia, peritajes, análisis de redes, preservación por las plataformas, alcance de

contenidos y valoración de indicios. En materia electoral, la prueba digital debe ser útil en plazos breves. Por otro lado, una regulación que establezca estándares técnicos altísimos puede volver impune la manipulación; una regulación que admita cualquier sospecha puede abrir la puerta a arbitrariedad. El punto de equilibrio será decisivo.

La ciberseguridad electoral también requiere desarrollo normativo y reglamentario. Deben establecerse obligaciones de gestión de riesgos, protocolos de incidentes, auditorías, pruebas de resiliencia, protección de bases de datos, capacitación de personal y coordinación con instituciones especializadas. Los principios clásicos de certeza y legalidad deben dialogar con la integridad tecnológica, la seguridad de sistemas y la confianza digital.

Retos democráticos

El principal reto democrático consiste en proteger la autonomía del voto en un entorno en el que la información puede ser fabricada, dirigida, amplificada y ocultada con precisión creciente. La democracia presupone que la ciudadanía decide a partir de razones, afectos, identidades, intereses y debates que pueden ser discutidos en común, es decir, que se trata de una ciudadanía informada. La comunicación algorítmica no elimina esa libertad, pero puede condicionarla si explota miedos, sesgos, vulnerabilidades o desinformación sin que las personas sepan que están siendo perfiladas.

La fragmentación del debate público será una preocupación de largo alcance. La microsegmentación permite que una campaña comunique mensajes distintos a públicos distintos. Esto puede mejorar la pertinencia de la información, pero también puede impedir el escrutinio colectivo. Cuando una promesa solo la ve un segmento y una amenaza solo circula ante otro, la ciudadanía deja de compartir una base común de deliberación. La democracia pierde capacidad para contrastar discursos y exigir coherencia.

La confianza pública puede erosionarse por dos vías: cuando las personas creen contenidos falsos y cuando dejan de creer en cualquier contenido porque todo podría ser falso. Este efecto de sospecha continua puede ser tan dañino como el engaño directo. Si la ciudadanía ya no sabe si un video, una voz, una imagen o una declaración son reales, la conversación pública se vuelve frágil. La justicia electoral debe proteger los hechos verificables, la autenticidad de los mensajes y una confianza mínima en el espacio público.

La alfabetización y la inclusión digital también serán parte de la agenda democrática. No todas las personas tienen las mismas capacidades para detectar la manipulación, usar herramientas de verificación, comprender etiquetas, identificar publicidad segmentada o proteger sus datos. Jóvenes, personas mayores, comunidades rurales, personas con discapacidad, población con menor acceso a la educación y grupos afectados por la brecha tecnológica pueden enfrentar riesgos distintos. La regulación debe acompañarse de alfabetización digital y accesibilidad. De lo contrario, la protección beneficiará más a quienes ya tienen ventajas.

La estabilidad electoral también depende del manejo de estos riesgos. Una campaña de desinformación en momentos cercanos a la jornada puede alterar percepciones, generar miedo, deslegitimar autoridades o sembrar dudas sobre resultados. Incluso cuando la información sea desmentida después, el daño puede permanecer. Las democracias deben desarrollar respuestas preventivas y cautelares respaldadas por una mayor capacidad técnica, porque el tiempo digital no coincide con los tiempos ordinarios del proceso jurisdiccional.

Implicaciones para la justicia electoral cercana

La IA y las plataformas digitales obligan a repensar la justicia electoral cercana. La cercanía ya no puede entenderse solo como presencia territorial, lenguaje claro o diálogo con comunidades. También debe incluir la capacidad de comprender el nuevo territorio digital en el que se forman preferencias, se disputan narrativas y se producen daños democráticos. El espacio público ya no está solo en plazas, medios, universidades o asambleas. También está en plataformas, anuncios segmentados, grupos de mensajería, buscadores, algoritmos y contenidos sintéticos.

Una justicia electoral cercana debe ser capaz de escuchar el territorio físico y el territorio digital. Debe comprender cómo circula una mentira, cómo se amplifica un ataque, cómo se segmenta un mensaje, cómo se manipula una imagen y cómo se construye una percepción pública. No para vigilar toda conversación, sino para proteger las condiciones mínimas de una deliberación libre. La cercanía, en esta materia, exige capacidad técnica y sensibilidad constitucional.

El TEPJF puede desempeñar un papel de articulación democrática al construir criterios que orienten a autoridades locales, partidos, plataformas, candidaturas y ciudadanía. Puede impulsar protocolos de prueba digital, promover criterios de etiquetado, exigir

transparencia en la publicidad política, proteger la libertad de expresión, sancionar manipulación acreditada y establecer límites al uso interno de IA. También puede fortalecer sus propias herramientas de comunicación para explicar a la ciudadanía qué riesgos digitales afectan sus derechos.

La justicia cercana también debe ser pedagógica y evitar que las sentencias sobre IA, plataformas digitales y elecciones queden encerradas en lenguaje técnico. Deben explicar por qué un contenido sintético importa, por qué la microsegmentación puede afectar la equidad, por qué un *deepfake* no es solo una mentira, por qué la libertad de expresión no protege la suplantación y por qué la regulación no debe convertirse en censura. La ciudadanía debe comprender las razones de la justicia electoral si se busca proteger la confianza pública.

En el fondo, la agenda de IA y plataformas digitales plantea un problema central para el futuro de la democracia mexicana. Si la voluntad ciudadana se forma en entornos opacos, personalizados, manipulables y controlados por actores con poder tecnológico, la justicia electoral deberá ampliar su mirada. No basta con proteger el voto cuando ya fue emitido. Es necesario proteger las condiciones que permiten que ese voto sea libre, informado y auténtico.

La justicia electoral cercana puede ofrecer una respuesta a esa transformación. Una justicia que entiende la tecnología sin rendirse ante ella, que protege la libertad sin tolerar engaños organizados, que usa herramientas digitales sin entregarles la decisión humana, que colabora con plataformas sin subordinarse a sus reglas privadas, que sanciona daños sin perseguir la crítica, que escucha a la ciudadanía, pero también comprende que los algoritmos moldean lo que la ciudadanía ve.

La agenda para la justicia electoral es, en suma, una agenda de confianza democrática. Confianza en que la información política puede ser discutida y no fabricada en secreto, en que las campañas no podrán explotar datos personales sin límites, en que las plataformas tendrán deberes frente a la democracia, en que la IA servirá como herramienta de apoyo y no como sustituto del juicio humano y, sobre todo, confianza en que el TEPJF podrá construir criterios para una época en la que la verdad pública, la identidad y la deliberación enfrentan formas nuevas de disputa.

El desafío es considerable, pero también abre una oportunidad. La justicia electoral mexicana puede anticiparse a una agenda que definirá los próximos ciclos democráticos. Puede construir una doctrina que proteja la autonomía del voto, la integridad informativa, la libertad de expresión, la equidad, la privacidad, la transparencia y la responsabilidad digital. Puede convertir el diálogo territorial en aprendizaje institucional.

Puede mostrar que la cercanía no consiste solo en acudir al territorio, sino en entender los espacios en los que hoy se juega la democracia.

Así entendida, la justicia electoral cercana en la era digital no es una justicia tecnocrática, es una justicia constitucional capaz de dialogar con la técnica para proteger mejor a la ciudadanía. Una justicia que sabe que detrás de cada dato hay una persona, detrás de cada algoritmo hay decisiones humanas, detrás de cada plataforma hay intereses y detrás de cada voto debe existir una voluntad libre. Esa es la tarea que este volumen deja abierta para el TEPJF y para el conjunto de instituciones democráticas mexicanas.



Conclusiones



Este volumen parte de una constatación que ya no puede ser tratada como una hipótesis de futuro: la democracia mexicana se desenvuelve en un entorno algorítmico. La ciudadanía se informa, conversa, duda, comparte, denuncia, se moviliza y decide en espacios atravesados por plataformas digitales, datos masivos, sistemas de recomendación, contenidos sintéticos, microsegmentación, inteligencia artificial (IA) generativa y redes de amplificación. Las elecciones ya no ocurren solo en casillas, campañas territoriales, debates públicos, *spots,* periódicos o plazas; también ocurren en pantallas, motores de búsqueda, grupos de mensajería, bibliotecas de anuncios, cuentas automatizadas, modelos predictivos y contenidos cuya autenticidad no siempre puede verificarse a simple vista.

Los diálogos regionales permitieron comprender que este cambio no es solo tecnológico, es un cambio en la cultura democrática, jurídica e institucional. La IA no modifica solo las herramientas disponibles para campañas o autoridades, también impacta en las condiciones conforme a las cuales se forma la voluntad ciudadana, se distribuye la información política, se atribuye la responsabilidad, se prueba una infracción y se protege la confianza pública. Por ello, el tema no puede quedar reservado a especialistas en datos o a empresas tecnológicas. Debe formar parte del núcleo de la justicia electoral contemporánea.

El aporte sustantivo del libro consiste en mostrar que la integridad electoral del siglo XXI exige mirar más allá de la jornada electoral. Durante mucho tiempo, la defensa de la elección se concentró en casillas, boletas, cómputos, financiamiento, tiempos oficiales, propaganda visible y resultados. Todo ello sigue siendo indispensable. Pero los seminarios mostraron que una elección también puede verse afectada antes de que la ciudadanía llegue a votar, cuando el entorno informativo se inunda de engaños, suplantaciones, imágenes sintéticas, mensajes segmentados, campañas encubiertas, violencia digital o publicidad opaca. Proteger el voto implica proteger también las condiciones que permiten formarlo con libertad.

Los diálogos permitieron ordenar una tensión que atravesó todas las sedes: la tecnología puede fortalecer la democracia y, al mismo tiempo, ponerla en riesgo. Puede facilitar la traducción, la accesibilidad, la búsqueda de precedentes, la educación cívica, el análisis de información, la detección de patrones anómalos y la comunicación institucional. Pero también puede producir contenidos verosímiles, amplificar ataques, simular respaldo ciudadano, explotar datos personales, ocultar propaganda, fragmentar el debate público y generar desconfianza sobre lo que se ve, se escucha o se lee. La conclusión no es que la IA deba prohibirse. La conclusión es que debe gobernarse con criterios democráticos.

Ese punto es central para evitar respuestas simples. La IA no es enemiga de la democracia por su sola existencia. Tampoco es una herramienta neutral que pueda dejarse a la lógica del mercado, de la innovación o de la estrategia electoral. Su impacto depende de quién la usa, con qué datos, con qué controles, con qué finalidad, con qué transparencia y con qué efectos. El derecho electoral debe distinguir entre el uso legítimo y el uso dañino. Entre creatividad política y engaño premeditado. Entre sátira y suplantación. Entre segmentación informativa y manipulación de vulnerabilidades. Entre apoyo institucional y sustitución del juicio humano.

El recorrido territorial aportó una lectura nacional que no habría podido construirse desde una sola sede. Tijuana abrió el debate desde la idea de democracia algorítmica y mostró que la equidad electoral debe pensarse también en términos de datos, plataformas y capacidad de segmentación. Arteaga llevó la discusión a la prueba, la trazabilidad, la autorregulación supervisada, la protección de datos y la necesidad de capacidades técnicas. Morelia colocó en el centro la ética digital, la ciudadanía crítica y la autenticidad de la comunicación pública. Campeche permitió discutir modelos comparados, estándares internacionales, responsabilidad de plataformas y riesgos de una regulación que puede proteger derechos o inhibir la expresión si se diseña sin cuidado. Tlaxcala aportó una mirada metodológica sobre el razonamiento jurídico, la prueba, las alucinaciones algorítmicas y los límites del uso de IA en tareas jurisdiccionales. Ciudad de México cerró el recorrido con una reflexión sobre gobernanza digital, moderación privada, bibliotecas de anuncios, redes inauténticas, colaboración con plataformas y responsabilidad institucional.

Como método deliberativo, los diálogos territoriales mostraron su valor. La justicia electoral cercana no solo consiste en llevar la voz del Tribunal Electoral del Poder Judicial de la Federación (TEPJF) a las regiones, también consiste en escuchar cómo cada región entiende los riesgos de la democracia digital. Una ciudad fronteriza observa

flujos de información, movilidad y tecnología desde una experiencia distinta a la de una universidad especializada en derechos humanos. Una sede con tradición académica puede enfatizar la ética y el pensamiento crítico. Una región con fuertes desafíos de conectividad puede insistir en la brecha digital y la accesibilidad. Una capital institucional puede mirar con mayor fuerza la relación con plataformas globales. Escuchar esas diferencias permite construir criterios con más contexto y con menor riesgo de abstracción.

El libro también aporta una advertencia sobre el lenguaje: el derecho, la tecnología y la ciudadanía no siempre hablan de lo mismo cuando usan las mismas palabras. Para una autoridad electoral, la prueba puede significar carga procesal, estándar de valoración y debido proceso. Para una plataforma, puede significar metadatos, trazabilidad, arquitectura de anuncios o criterios de moderación. Para la ciudadanía, puede significar saber si aquello que vio es real o falso. Sin un lenguaje común, la regulación será débil, la prueba será lenta, la colaboración será incompleta y la pedagogía pública será insuficiente. La justicia electoral del futuro deberá ser interdisciplinaria por necesidad, no por moda.

Lo que sigue para el TEPJF es una agenda exigente en la que deberá resolver controversias sobre contenidos generados con IA; *deepfakes*; imágenes sintéticas de niñas, niños y adolescentes; violencia política digital; calumnia; suplantación de identidad; publicidad segmentada; uso de datos personales; cuentas inauténticas; propaganda encubierta; anonimato; plataformas sin representación local; fiscalización de pauta digital, y responsabilidad de actores que intervienen en cadenas complejas de producción y difusión de contenidos. Cada uno de estos casos obligará a adaptar categorías existentes y, en algunos ámbitos, a construir criterios nuevos.

Esa tarea jurisdiccional no puede renunciar a la libertad de expresión. La democracia necesita crítica, sátira, humor, denuncia, debate intenso y circulación abierta de ideas. La regulación de la comunicación digital no puede convertirse en censura preventiva ni en control general de contenidos. Pero tampoco puede aceptar que cualquier conducta quede protegida con el argumento de libertad de expresión. La suplantación, la desinformación intencionada, la propaganda encubierta, la manipulación de datos, la violencia política y el uso de contenidos sintéticos para engañar a la ciudadanía requieren una respuesta institucional. La clave será construir criterios proporcionados, centrados en daño, dolo, contexto, alcance, financiamiento, coordinación y afectación real de derechos o condiciones de competencia.

El impacto para el futuro de la democracia mexicana será profundo. La IA puede mejorar la participación pública si se usa para acercar información, hacer accesibles

las sentencias, traducir contenidos, comparar propuestas, detectar contradicciones, explicar derechos y ampliar capacidades ciudadanas. Pero puede debilitar la democracia si convierte a la ciudadanía en objeto de perfilamiento, si fragmenta el debate común, si permite que cada persona reciba una versión distinta de la realidad, si facilita campañas de miedo o si erosiona la confianza en cualquier evidencia. La democracia necesita hechos discutibles, no realidades fabricadas para cada segmento.

Uno de los riesgos más graves no es solo que la ciudadanía crea algo falso, sino que deje de creer en todo. La proliferación de contenidos sintéticos puede producir una sospecha general sobre la autenticidad de la información pública. Si todo video puede ser falso, toda voz puede ser fabricada y toda imagen puede ser simulada, entonces la deliberación democrática pierde un punto de apoyo. La justicia electoral debe ayudar a preservar un mínimo de confianza en la conversación pública. No para imponer una verdad oficial, sino para proteger condiciones de autenticidad, transparencia y responsabilidad.

Es importante que la justicia electoral considere que no todas las personas enfrentan los riesgos digitales en las mismas condiciones. Las brechas relacionadas con la conectividad, la edad, la educación, la discapacidad, la lengua, el ingreso y la alfabetización tecnológica pueden hacer que ciertos grupos sean más vulnerables frente a manipulación, fraude informativo o violencia digital. La educación cívica del siglo XXI debe incorporar la verificación de fuentes, el reconocimiento de contenidos sintéticos, la comprensión de la publicidad segmentada, el cuidado de los datos personales y la denuncia de prácticas abusivas. Una ciudadanía crítica es tan necesaria como una autoridad capaz de sancionar.

La justicia electoral cercana, en este sentido, debe proteger las condiciones constitucionales del debate electoral. Debe intervenir cuando existan usos de la tecnología capaces de afectar derechos, equidad, información pública, dignidad, autonomía del voto o confianza en el proceso. Debe hacerlo con método, con prueba y con proporcionalidad. La velocidad digital no justifica decisiones sin fundamento, pero la lentitud institucional tampoco puede ser excusa para dejar que el daño se consume.

Asimismo, las sentencias sobre IA y plataformas digitales deberán explicar por qué un contenido sintético puede afectar una elección, por qué la microsegmentación puede erosionar la equidad, por qué una plataforma privada tiene deberes democráticos, por qué un *deepfake* no es solo una mentira y por qué regular no significa censurar. Si la ciudadanía no entiende estas razones, las decisiones pueden parecer arbitrarias, tecnocráticas o lejanas. Una justicia cercana debe traducir la complejidad sin empobrecer el razonamiento.

También será necesario comparar experiencias internacionales sin copiar modelos de forma acrítica. México necesita aprender de otros sistemas, pero construir respuestas adecuadas a su marco constitucional, a su pluralidad social y a sus capacidades institucionales.

La conclusión general del volumen es que la democracia mexicana no puede enfrentar la IA con miedo ni con ingenuidad. Debe hacerlo con derecho, técnica, pedagogía, ética y deliberación pública. La justicia electoral cercana ofrece un camino para esa tarea. No porque tenga todas las respuestas, sino porque parte de una convicción adecuada. Para proteger la democracia hay que escuchar cómo cambia. Para juzgar los conflictos del presente hay que comprender los lenguajes del presente. Para sostener la confianza en el futuro hay que construir instituciones capaces de ver, probar, explicar y decidir en una época en la que la realidad pública puede ser fabricada con una facilidad inédita.



Referencias



Acuerdo INE/JGE175/2025, Junta General Ejecutiva del Instituto Nacional Electoral. (2025). https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/184916/JGEor202508-20-ap-5-2.pdf

Artículo 19. (2024). Autoridades electorales, plataformas digitales y democracia en México. https://articulo19.org/autoridades-electorales-plataformas-digitales-y-democracia-en-mexico/

Bayer, J. (2020). Double harm to voters: data-driven micro-targeting and democratic public discourse, *Internet Policy Review*, *9*(1). https://doi.org/10.14763/2020.1.1460

Cebrián Beltrán, S. (2024). De la talla única al traje a medida: perfiles constitucionales del microtargeting político para influir en las elecciones. *Cortes*. *Anuari de Dret Parlamentari*, (38), 287-310. https://www.cortsvalencianes.es/sites/default/files/media/file_author/00_A38_III_02.pdf

Channel 4 News. (2020). Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016. https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016

Communications Decency Act of 1996, 47 U.S.C. § 230, United States Congress. (1996).

Dartmouth University. (1956). Dartmouth Summer Research Project on Artificial Intelligence. https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth

Davis, K. (2025). A Case for Regulating Political Microtargeting: How the Messaging of Meta Ads in the 2024 U.S. Presidential Election Varied by Age, Gender, and State. Tesis de licenciatura. University of Chicago. https://knowledge.uchicago.edu/records/349e1-dhv09

Del Pozo, C. y Rojas Arroyo, D. (2024). IA Generativa y su influencia en las elecciones de México 2024. Friedrich-Naumann-Stiftung für die Freiheit. https://www.freiheit.org/es/publikation/ia-generativa-y-su-influencia-en-las-elecciones-de-mexico-2024

El Heraldo de México. (2025, 21 de mayo). El TEPJF impulsa la innovación tecnológica en la justicia electoral con inteligencia artificial. https://heraldodemexico.com.mx/edicion-impresa/2025/5/21/el-tepjf-impulsa-la-innovacion-tecnologica-en-la-justicia-electoral-con-inteligencia-artificial-700811.html

Elections Modernization Act, Canadá. (2019). https://www.parl.ca/DocumentViewer/en/42-1/bill/C-76/first-reading

Fernández Gibaja, A. (2017). Protecting democracy from technology and big data, International Institute for Democracy and Electoral Assistance. https://www.idea.int/news/protecting-democracy-technology-and-big-data

Foos, F. (2024). The use of AI by election campaigns. LSE *Public Policy Review*, *3*(3), 1-7. https://ppr.lse.ac.uk/articles/10.31389/lseppr.112

Google Cloud. (2026). Inteligencia artificial: una guía fácil de entender. https://cloud.google.com/learn/what-is-artificial-intelligence?hl=es-419#types-of-artificial-intelligence

Honest Ads Act, Congreso de los Estados Unidos de América. (2023). https://www.congress.gov/bill/118th-congress/senate-bill/486

Iniciativa con Proyecto de Decreto por el que se Expide la Ley Federal para el Desarrollo Ético Soberano e Inclusivo de la Inteligencia Artificial en México, Cámara de Diputados. (2025). https://sil.gobernacion.gob.mx/Archivos/Documentos/2025/04/asun_4896460_20250430_1747757009.pdf

Iniciativa con Proyecto de Decreto por el que se Expide la Ley para la Regulación Ética de la inteligencia Artificial y la robótica, Cámara de Diputados. (2023). https://sil.gobernacion.gob.mx/Archivos/Documentos/2023/05/asun_4572130_20230524_1684946286.pdf

Iniciativa con Proyecto de Decreto por el que se Expide la Ley que crea la Agencia Mexicana para el Desarrollo de la Inteligencia Artificial. (2023). https://sil.gobernacion.gob.mx/Archivos/Documentos/2023/12/asun_4673074_20231205_1697051780.pdf

Iniciativa con Proyecto de Decreto por el que se Expide la Ley que Regula el Uso de la Inteligencia Artificial. (2023). https://infosen.senado.gob.mx/sgsp/gaceta/65/3/2023-11-28-1/assets/documentos/Ini_Sen_Gustavo_Madero_Ley_que_Regula_el_Uso_de_la_IA.pdf

Iniciativa con Proyecto de Decreto por el que se Expide Ley Federal que Regula la Inteligencia Artificial, Cámara de Senadores. (2023). https://sil.gobernacion.gob.mx/Archivos/Documentos/2024/04/asun_4729480_20240402_1712079223.pdf

Instituto Nacional de Estadística y Geografía. (2025). Encuesta Nacional sobre Disponibilidad y Uso de la Información en los Hogares (ENDUTIH). https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2025/endutih/ENDUTIH_24_RR.pdf

Integridad de la Publicidad en Línea, República de Singapur. (2024). https://sso.agc.gov.sg/Acts-Supp/34-2024/Published/20241121?DocDate=20241121

International Institute for Democracy and Electoral Assistance y Fundação Getulio Vargas Comunicacao. (2025). Artificial Intelligence and Information Integrity: Latin American Experiences. Policy Paper No. 34. https://www.idea.int/publications/catalogue/artificial-intelligence-and-information-integrity-latin-american-experiences

International Institute for Democracy and Electoral Assistance. (2011). *Una introducción al voto electrónico: consideraciones esenciales*. Policy Paper. https://www.idea.int/sites/default/files/publications/una-introduccion-al-voto-electronico.pdf

International Institute for Democracy and Electoral Assistance. (2020). *Online political advertising and microtargeting: The latest legal, ethical, political and technological evolutions*. Webinar Series Report. https://www.idea.int/publications/catalogue/online-political-advertising-and-microtargeting-latest-legal-ethical

International Institute for Democracy and Electoral Assistance. (2024). *La inteligencia artificial para la gestión electoral*. https://www.idea.int/sites/default/files/2024-10/inteligencia-artificial-para-la-gestion-electoral.pdf

International Organization for Standardization. (2026). Inteligencia artificial: qué es, cómo funciona y por qué es importante. https://www.iso.org/es/inteligencia-artificial

Jungherr, A., Rauchfleisch, A. y Wuttke, A. (2026). Artificial Intelligence in Election Campaigns: Perceptions, Penalties, and Implications. *Political Communication*, *43*(4), 585-606. https://www.tandfonline.com/doi/full/10.1080/10584609.2025.2611913

Jurisprudencia 13/2024, Tribunal Electoral del Poder Judicial de la Federación. (2024). https://www.te.gob.mx/ius2021/#/13-2024

Klosowski, T. (2024). How political campaigns use your data to target you. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2024/04/how-political-campaigns-use-your-data-target-yo

Ley Electoral de Brasil n.º 9.504/1997, Congreso Nacional de Brasil. (1997). https://www.planalto.gov.br/ccivil_03/leis/l9504.htm

Matsumi H. y Solove, D. J. (2025). The Prediction Society: AI and the Problems of Forecasting the Future. *2025 Illinois Law Review*, *2025*(1), 1-62. https://illinoislawreview.org/wp-content/uploads/2025/02/Solove-2.pdf

Microsoft. (2026a). ¿Qué es la inteligencia artificial? https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-artificial-intelligence#types-of-ai

Microsoft. (2026b). What is an AI platform? https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-an-ai-platform

National Aeronautics and Space Administration. (2026). What is Artificial Intelligence? https://www.nasa.gov/what-is-artificial-intelligence/

Noble, S. U. (2018). Algorithms of oppression: How search engines reinforce racism. NYU Press.

Noetzel, S., Binder, A. y Matthes, J. (2024). More than meets the eye: Understanding political microtargeting processing with gaze-cued retrospective think-aloud methodology, *Media and Communication*, *12,* artículo 8679. https://doi.org/10.17645/mac.8679

Okidegbe, N. (2025). How not to democratize algorithms. *Wisconsin Law Review*, Wisconsin, 895. https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=5185&context=faculty_scholarship

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2026). UNESCO and AI. https://www.unesco.org/en/query-list/a/ai#term-definition

Organización para la Cooperación y el Desarrollo Económico. (2024). Marco para la Gobernanza Anticipatoria de las Tecnologías Emergentes. https://www.oecd.org/en/publications/framework-for-anticipatory-governance-of-emerging-technologies_0248ead5-en.html

Ramírez Plascencia, D., Ochoa Zuno, A., y Alonzo González, R. M. (2025). Digital Partisans: An Inquiry on the Use of Bots for Political Propaganda in Mexico. *Teknokultura*, *22*(2), 175-184. https://revistas.ucm.es/index.php/TEKN/es/article/view/97497/4564456572253

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, *Diario Oficial de la Unión Europea*. (2024). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202401689

Reglamento 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política, *Diario Oficial de la Unión Europea*. (2024). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202400900

Reglas para la protección de niñas, niños y adolescentes en materia de propaganda y mensajes electorales para el Proceso Electoral Extraordinario del Poder Judicial de la Federación 2024-2025, Instituto Nacional Electoral. (2025). https://

repositoriodocumental.ine.mx/pdfjs-flipbook/web/viewer.html?file=/xmlui/bitstream/handle/123456789/179066/Anexo-1-Reglas-PEEPJF-menores.pdf

Resolución TSE n.º 23.610/2019, Tribunal Superior Electoral de Brasil. (2019). https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019

Rojas, D. (2024). ¿Debe el INE aplicar el artículo 41 a las plataformas digitales? Agencia Brunch. https://www.agenciabrunch.com/debe-el-ine-aplicar-el-articulo-41-a-las-plataformas-digitales

Romero Flores, R. y Téllez Valdés, J. (2010). *Voto electrónico, derecho y otras implicaciones*. Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas. http://ru.juridicas.unam.mx/xmlui/handle/123456789/11711

Rubinstein, I. S. (2014). Voter privacy in the age of big data. *Wisconsin Law Review*, *2014*(5), pp. 861-936. https://wlr.law.wisc.edu/wp-content/uploads/sites/701/2015/02/1-Rubinstein-Final-Online.pdf

Russell, S. y Norving, P. (2020). *Artificial intelligence: A modern approach*. Pearson.

Saura García, C. (2023). El big data en los procesos políticos: hacia una democracia de la vigilancia. *Revista de Filosofía*, *80*, 215-232. http://dx.doi.org/10.4067/S0718-43602023000100215

Sentencia SRE-PSD-15/2025, Tribunal Electoral del Poder Judicial de la Federación. (2025). https://www.te.gob.mx/media/SentenciasN/pdf/especializada/SRE-PSD-0015-2025.pdf

Sentencia SRE-PSL-19/2025, Tribunal Electoral del Poder Judicial de la Federación. (2025). https://www.te.gob.mx/media/SentenciasN/pdf/especializada/SRE-PSL-0019-2025.pdf

Sentencia SUP-RAP-172/2021, Tribunal Electoral del Poder Judicial de la Federación. (2021). https://www.te.gob.mx/sentenciasHTML/convertir/expediente/SUP-RAP-0172-2021

Sentencia SUP-RAP-41/2012, Tribunal Electoral del Poder Judicial de la Federación (2012). https://www.te.gob.mx/media/SentenciasN/pdf/Superior/SUP-RAP-0041-2012.pdf

Sentencia SUP-REP-542/2015 y SUP-REP-544/2015 acumulados, Tribunal Electoral del Poder Judicial de la Federación. (2015). https://www.te.gob.mx/sentenciasHTML/convertir/expediente/SUP-REP-0542-2015

Sentencia SUP-REP-893/2024 y acumulado, Tribunal Electoral del Poder Judicial de la Federación. (2024) https://www.te.gob.mx/media/SentenciasN/pdf/superior/SUP-REP-0893-2024.pdf

Sentencia SUP-REP-893/2024 y SUP-REP-900/2024, Acumulado, Tribunal Electoral del Poder Judicial de la Federación. (2024). https://www.te.gob.mx/media/pdf/9dbb7744a206178.pdf

Simon, F. y Altay, S. (2025). *Don't panic (yet): Assessing the evidence and discourse around generative* AI *and elections*. Knight First Amendment Institute, Columbia University. https://knightcolumbia.org/content/dont-panic-yet-assessing-the-evidence-and-discourse-around-generative-ai-and-elections

Swissinfo. (2026). El tribunal electoral de Brasil limita el uso de propaganda hecha con IA en los comicios. https://www.swissinfo.ch/spa/el-tribunal-electoral-de-brasil-limita-el-uso-de-propaganda-hecha-con-ia-en-los-comicios/91026286

Tratado entre México, Estados Unidos y Canadá, Gobierno de México. (2020, 1 de julio). https://www.gob.mx/t-mec/acciones-y-programas/textos-finales-del-tratado-entre-mexico-estados-unidos-y-canada-t-mec-202730?state=published

Tribunal Electoral del Poder Judicial de la Federación. (2022). Voto en el extranjero y nuevas tecnologías. Colección TEPJF. https://biblio.juridicas.unam.mx/bjv/detalle-libro/6142-voto-en-el-extranjero-y-nuevas-tecnologias-coleccion-tepjf

Valdés Zurita, L. (2022). Modelo de comunicación político-electoral. En Saúl López Noriega (coord.), *Manual de periodismo judicial electoral* (pp. 32-33). Tribunal Electoral del Poder Judicial de la Federación.

Zuboff, S. (2019), *La era del capitalismo de la vigilancia: la lucha por un futuro humano frente a las nuevas fronteras del poder* (Marcos Pérez Sánchez, trad.). Paidós.

Zuiderveen Borgesius, F., Möller, J., Kruikemeier, S., Fathaigh, R., Irion, K., Dobber, T. Bodo, B. y Vreese, C. de. (2018). Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review*, *14*(1). https://doi.org/10.18352/ulr.420

Bibliografía sugerida

Bennett, C. J. y Gordon, J. (2021). Understanding the "micro" in political micro-targeting: An analysis of Facebook digital advertising in the 2019 federal Canadian election. *Canadian Journal of Communication*, *46*(3), 431-459. https://doi.org/10.22230/cjc.2021v46n3a3815

Cleary, S., Connor, H. y Navin, M. (2026). *AI-generated evidence is a threat to public trust in the courts*. National Center for State Courts. https://www.ncsc.org/resources-courts/ai-generated-evidence-threat-public-trust-courts

De-Santis, A., Torres-Toukoumidis, A. y Morejon-Vallejo, R. (2026). Artificial intelligence in political communication and citizens' perceptions of disinformation and democratic legitimacy in Ecuador. *Social Sciences & Humanities Open*, *13*. https://www.sciencedirect.com/science/article/pii/S2590291126001269

Flores-Saviaga, C. y Savage, S. (2019). *Anti-Latinx computational propaganda in the United States*. Institute of the Future White Paper. https://arxiv.org/pdf/1906.10736

Iniciativa con proyecto de decreto por el que se reforman los artículos 4, 6, 25, 26 y 73 de la Constitución Política de los Estados Unidos Mexicanos, en Materia de Reconocimiento de los Ecosistemas Digitales e Inteligencia Artificial, Cámara de Diputados. (2026). https://sil.gobernacion.gob.mx/Archivos/Documentos/2026/04/asun_5063710_20260414_1771376904.pdf

Kalsnes, B. y Schia, N. N. (2026). *Protecting democracy: Comparing codes of conduct for generative* AI *use during elections*. Information, Communication & Society. https://doi.org/10.1080/1369118X.2026.2647362

May Grosser, S. (2025). Diputada del PUSC propone regular uso de inteligencia artificial en procesos electoral. Delfino. https://delfino.cr/2025/03/diputada-del-pusc-propone-regular-uso-de-inteligencia-artificial-en-procesos-electorales

Ranka, H., Surana, M., Kothari, N., Pariawala, V., Banerjee, P., Surve, A., Reddy Sankepally, S., Jain, R., Lalwani, J. y Mehta, S. (2024). Examining the implications of deepfakes for election integrity. *Computers and Society*, June.

Red de Conocimientos Electorales-Aceproject. (2026). Administración y costo de elecciones. Elecciones y tecnología. http://www.aceproject.org/main/espanol/et/et30.html

Van Gils, F., Müller, W. y Prüfer, J. (2025). Microtargeting, voters' unawareness, and democracy. *Journal of Law, Economics, and Organization*, *41*(2), 634-653. https://doi.org/10.1093/jleo/ewae002

Yan, H. Y., Morrow, G., Yang, K. y Wihbey, J. (2025). The origin of public concerns over AI supercharging misinformation in the 2024 U.S. presidential election. *Harvard Kennedy School Misinformation Review*, *6*(1). https://doi.org/10.37016/mr-2020-171

Zhu, J. y Isaacs, R. (2024). Campaign microtargeting and AI can jeopardize democracy. *LSE British Politics and Policy*. https://blogs.lse.ac.uk/politicsandpolicy/campaign-microtargeting-and-ai-can-jeopardize-democracy/



Anexo metodológico



La colección *Justicia electoral cercana: diálogos sobre nuestra democracia* es resultado de un proyecto institucional, académico y de la sociedad civil, impulsado por el Tribunal Electoral del Poder Judicial de la Federación (TEPJF) y la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES). El punto de partida fue la organización de seis seminarios, en diferentes regiones del país, para abordar algunos de los principales debates de la justicia electoral en México y otras democracias. Un propósito central de estos seminarios consistió en que su dinámica reuniera las condiciones adecuadas para un diálogo genuino que permitiera un intercambio libre y propositivo de ideas, enfoques y reflexiones, bajo la premisa de que la democracia se vive de manera diferente a lo largo del vasto y diverso territorio mexicano.

La colección *Justicia electoral cercana* se integra, de esta manera, por cuatro volúmenes, acorde a los temas que se abordaron en cada uno de los seminarios regionales:

1) Del litigio al diálogo en la justicia electoral. Mecanismos alternativos, mediación y paz democrática.
2) Elecciones judiciales en México. El nuevo paradigma democrático.
3) Representación, inclusión y pluralismo. Pueblos indígenas, grupos de atención prioritaria y justicia electoral.
4) Democracia entre algoritmos. Inteligencia artificial, plataformas digitales y justicia electoral.

Estructura del libro

Este libro se divide en dos grandes secciones. La primera ofrece una introducción y un análisis jurídico del tema en cuestión, exponiendo sus principales coordenadas teóricas y conceptuales, así como su diseño jurídico nacional y convencional de acuerdo con la Constitución, instrumentos internacionales, regionales,

legislación, precedentes judiciales y criterios jurisprudenciales correspondientes. De tal manera que este apartado permite conocer y analizar sus principales antecedentes, categorías jurídicas, problemas interpretativos, criterios jurisdiccionales y tensiones o riesgos democráticos.

La segunda parte corresponde al procesamiento analítico de los diálogos celebrados en las seis regiones. Este es el núcleo del libro, pues sistematiza las discusiones sostenidas en cada seminario, al identificar y ordenar los principales problemas jurídicos, tensiones institucionales y propuestas de políticas públicas que surgieron en las mesas de trabajo. Para elaborar esta segunda sección se utilizaron como insumos las relatorías de cada mesa, las transcripciones de los diálogos, así como las preguntas detonadoras. Además, para sistematizar las aportaciones de los diálogos se utilizaron modelos de inteligencia artificial (IA) generativa como herramientas auxiliares para ordenar información, identificar patrones temáticos, comparar regiones y agrupar problemas recurrentes. Este apoyo tecnológico no sustituyó el criterio editorial, jurídico ni académico del equipo responsable; por el contrario, fue utilizado bajo supervisión humana, con revisión, depuración, contraste y edición sustantiva de los contenidos.

Sedes y fechas de los seminarios regionales

Los seminarios se llevaron a cabo en seis regiones del país, con el objetivo de conocer, escuchar y entender mejor la diversidad de perspectivas de estos temas en el territorio mexicano. Las sedes y fechas fueron las siguientes:

1) Tijuana, Baja California, 30 de abril de 2026. Universidad Autónoma de Baja California.
2) Arteaga, Coahuila, 14 de mayo de 2026. Academia Interamericana de Derechos Humanos.
3) Morelia, Michoacán, 21 de mayo de 2026. Universidad Michoacana de San Nicolás de Hidalgo.
4) San Francisco de Campeche, Campeche, 28 de mayo de 2026. Universidad Autónoma de Campeche.
5) Tlaxcala de Xicohténcatl, Tlaxcala, 4 de junio de 2026. Universidad Autónoma de Tlaxcala.

6) Ciudad de México, 15 de junio de 2026. Universidad Autónoma Metropolitana – Rectoría General.

Diseño y dinámica de las mesas de diálogo

En cada seminario se realizaron cuatro mesas de trabajo simultáneas, una por cada eje temático de la colección. Esto permitió que en cada sede hubiese un diálogo especializado, pero bajo una estructura metodológica común. Cada mesa contó con los siguientes perfiles:

1) Una persona moderadora, encargada de presentar el tema, explicar la metodología, ordenar las intervenciones, administrar tiempos y conducir el cierre.
2) Una persona secretaria de estudio y cuenta del TEPJF, designada para presentar el debate desde la perspectiva jurisdiccional.
3) Personas ponentes provenientes de la academia, sociedad civil o ámbitos técnicos especializados, seleccionadas por su experiencia en el tema correspondiente.
4) Personas participantes de la mesa, con el perfil de integrantes de instituciones electorales, universidades, organizaciones sociales, estudiantes, personas servidoras públicas y ciudadanía.
5) Una persona relatora, responsable de registrar los argumentos, propuestas, consensos y desacuerdos, así como de exponer una síntesis estructurada al cierre de la mesa.

Esta integración de las mesas buscó equilibrar tres perspectivas: la jurisdiccional, la académica y la social. Esta combinación fue clave para uno de los objetivos de la colección: elaborar una relatoría analítica que no fuera solo una memoria de intervenciones, sino una sistematización de problemas públicos, argumentos jurídicos y propuestas institucionales.

Preguntas detonadoras

Las preguntas detonadoras fueron incorporadas como herramientas orientativas del diálogo, sin que estas implicaran límite alguno. En este sentido, su función fue abrir

la discusión, plantear problemas comunes y permitir que las intervenciones se desarrollaran desde la experiencia regional. Las preguntas detonadoras propias de este volumen, *Democracia entre algoritmos. Inteligencia artificial, plataformas digitales y justicia electoral*, fueron las siguientes:

1) ¿Cómo impactan la tecnología y la IA en la labor jurisdiccional electoral?
2) ¿Cuál es el alcance del control jurisdiccional sobre plataformas privadas en procesos electorales?
3) ¿Qué límites deben aplicarse a la propaganda política generada mediante IA?
4) ¿Cuáles son los criterios más efectivos para sancionar la posible desinformación intencionada?
5) ¿Cómo afecta la microsegmentación política en el discurso digital a la igualdad de la contienda, especialmente ante la recolección masiva de datos, la clasificación de audiencias y los mensajes políticos diferenciados?
6) ¿Qué capacidades institucionales requiere el Estado para enfrentar la manipulación digital del voto?

Metodología y colaboraciones

La metodología se pensó para asegurar una construcción colectiva de cada uno de los volúmenes de la colección. Son libros elaborados por un amplio número de personas con el ánimo de contrastar la perspectiva académica, jurídica y ciudadana frente a la realidad de los diversos contextos nacionales. El valor de esta metodología reside en que cada volumen hace un esfuerzo por dialogar con las diferentes problemáticas del país. Cada sede ofreció un contexto distinto, que se reflejó en las experiencias que aportaron las personas participantes. En este sentido, esta colección busca contribuir a una justicia electoral cercana, es decir, que escucha, dialoga y aprende de la pluralidad del país. Las personas que contribuyeron a la elaboración de este volumen —ya fuera mediante la participación en los diálogos, la moderación de las discusiones, el análisis de precedentes judiciales o la relatoría de lo más relevante de cada mesa— son las siguientes:

1) Juan José Bautista González
2) Julio César Barreto Ariza

3) José Rafael Belandria García
4) Romina Chávez Nava
5) Mauricio Del Toro Huerta
6) Fernando Enrique Domínguez Salazar
7) Brenda Durán Soria
8) Fernando Anselmo España García
9) Jonathan Samuel Flores Pertuz
10) Leopoldo Gama Leyva
11) José Eduardo González Rodríguez
12) Hugo Gutiérrez Trejo
13) Pablo Hernández Márquez
14) María Guadalupe Imormino de Haro
15) Ana Ximena Jacoby
16) Pedro López Malo Lara
17) Jorge Omar López Penagos
18) Luis Arturo Monroy Abunáder
19) Emmanuel Montiel Vázquez
20) Adriana Morales Torres
21) Alma Beatriz Navarro Cerda
22) Gabriela Ibeth Navarro Díaz de León
23) Alejandra Olvera Dorantes
24) Javier Miguel Ortiz Flores
25) Paul Alexis Ortiz Vázquez
26) Yaqueline Pech Huh
27) Víctor Manuel Pérez Chávez
28) Karina Pérez Dorsey
29) Eliana Pérez Gaffney
30) Rafael Gerardo Ramos Córdova
31) Gloria Sthefanie Rendón Barragán
32) Anselmo Rodríguez Parra
33) Víctor Hugo Rojas Vásquez
34) Enrique Rovelo Espinosa
35) Martin Cutberto Vera Martínez
36) Karen Elizabeth Vergara Montufar



Justicia electoral cercana: diálogos sobre nuestra democracia
Volumen IV. *Democracia entre algoritmos. Inteligencia artificial, plataformas digitales y justicia electoral*
se terminó de imprimir en octubre de 2026
en la Dirección General de Documentación
del Tribunal Electoral del Poder Judicial de la Federación.

Su tiraje fue de 100 ejemplares.

Editorial TEPJF Sí, también hacemos LIBROS

Democracia entre algoritmos explora cómo la inteligencia artificial y las plataformas digitales han transformado el espacio en el que se forma la voluntad ciudadana y se debate en la esfera pública. Detrás de cada algoritmo hay decisiones humanas; detrás de cada dato, una persona; detrás de cada plataforma, reglas privadas e intereses económicos. Este volumen sostiene que la justicia electoral debe comprender ese ecosistema para proteger derechos, equidad y confianza pública, distinguiendo entre usos legítimos y dañinos de la tecnología. Con aportaciones sobre prueba digital, responsabilidad de plataformas, contenidos sintéticos y educación cívica digital, el Tribunal Electoral del Poder Judicial de la Federación y la Asociación Nacional de Universidades e Instituciones de Educación Superior ofrecen una reflexión indispensable para pensar una justicia electoral capaz de gobernar la tecnología sin someterse a ella.