

Recomendaciones para combatir la desinformación frente a los procesos electorales en Colombia

1. Contexto: El vínculo entre la desinformación y la privacidad

La desinformación impulsada por internet y el uso de las redes sociales supone un desafío que muchos hacedores de políticas están abordando o están dispuestos a abordar. En internet, la desinformación es cada vez más personalizada. Este fenómeno es tan preocupante que [ha sido identificado como uno de los principales riesgos globales a corto y mediano plazo](#).

En tiempos de la IA generativa, donde el costo económico y la dificultad técnica que supone la producción y difusión de contenido de desinformación se ha reducido notablemente, la preocupación por el impacto de la desinformación va en aumento. Mientras tanto, la privacidad online y la protección de los datos personales son una agenda inconclusa en América Latina.

Existe una conexión entre la capacidad de recolectar y procesar grandes cantidades de datos personales y la forma en la que se crea y divulga contenido de desinformación en redes sociales y aplicaciones de mensajería en lo particular y en internet en lo general. La desinformación se [concreta](#) cuando se divulga contenido falso inexacto o descontextualizado con la intención de manipular.

[El fenómeno de la desinformación es anterior al surgimiento de internet](#). Pero es gracias al surgimiento de las nuevas tecnologías que su generación y propagación mejora. Esto se apoya en el propio modelo económico que sustenta a las plataformas escalando su efectividad y alcance. Por un lado, las redes sociales poseen algoritmos de recomendación de contenidos que se sirven de los datos personales para generar perfiles a los que luego pueden presentar contenidos publicitarios segmentados, incluyendo propaganda explícitamente política. Esta técnica se conoce como “microtargeting”.

El [microtargeting político busca impactar directa o indirectamente en la democracia](#). Se utiliza para convencer a los votantes, incentivar o desincentivar la participación en las urnas o para recaudar fondos con información deliberadamente sacada de contexto, inexacta o errónea.

El control que ejercen estas compañías plantea serias [preocupaciones sobre los derechos de los usuarios](#). Al tener acceso a cantidades masivas de información personal, estas empresas tienen la capacidad de moldear el contenido que los usuarios ven e interactúan, pudiendo presentar contenido altamente personalizado a cada persona. Esto se hace a través de construir perfiles que pueden revelar hábitos, relaciones sociales, preferencias políticas y opiniones, por mencionar algunos ejemplos. Los datos personales son el combustible que

potencia la desinformación hoy en día, ya sea que hayan sido provistos por el propio usuario o generados por las plataformas a partir de sus interacciones en internet.

Para los actores de la desinformación, el acceso a herramientas sofisticadas, como las utilizadas para crear “deepfakes” mediante IA generativa o “bots” programados para manipular contenido, potencia la efectividad de este *microtargeting*, dificultando su detección.

Por esta razón, la aplicación de leyes y políticas estrictas en materia de protección de datos personales y privacidad permiten reducir el impacto que tiene el contenido falso o manipulativo. Esto es especialmente importante en contextos electorales, donde la desinformación impacta y empobrece el debate público, afectando de forma directa los derechos políticos y electorales.

Desde las organizaciones firmantes señalamos la aplicación de leyes de protección de datos personales y a las políticas de privacidad como un mecanismo eficiente para mejorar la calidad de nuestras democracias y reducir la manipulación del discurso público en entornos digitales y su impacto en contextos electorales.

2. Recomendaciones

La desinformación es un fenómeno particularmente visible en contextos electorales. Desde Argentina hasta México, pasando por Brasil, Colombia o Perú, muchos países de América Latina tendrán procesos electorales relevantes en los próximos años.

Brindar a la ciudadanía información de calidad y de diferentes fuentes es un elemento esencial para el ejercicio de los derechos políticos. A los fines de resguardar en la medida de lo posible el proceso electoral, estos países deben hacer valer sus leyes de privacidad y de protección de datos personales a través de sus autoridades competentes, en sintonía con los poderes judiciales y tribunales electorales.

Desde la sociedad civil, en conjunto con la Defensoría del Pueblo en el marco del [compromiso con un proceso electoral libre y en paz en Colombia](#), ofrecemos las siguientes recomendaciones para combatir el fenómeno de la desinformación a partir de la protección de los datos personales durante los contextos electorales.

RECOMENDACIONES DE EJECUCIÓN INMEDIATA A PARTIR DE LO PREVISTO POR LA LEY 1581 Y LA CIRCULAR 02/2026 DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

1. La autoridades deben cumplir y hacer cumplir el marco legal (Ley 1581 de 2012 y Circular 02 de 2026 de la SIC), con directrices estrictas y auditorías dirigidas a partidos

políticos, candidatos, empresas de marketing electoral y cualquier organización que trate datos personales a los fines de comunicar contenido electoral. Estas medidas deben estar dirigidas a garantizar la privacidad de los ciudadanos. Tanto la Superintendencia de Industria y Comercio (SIC) como el Consejo Nacional Electoral (CNE) deben ejercer supervisión activa, con mecanismos de denuncia accesibles para la ciudadanía y sanciones efectivas, con el respeto del debido proceso y otros derechos fundamentales, que disuadan el incumplimiento.

- a. Las autoridades responsables de supervisar la protección de datos personales y en materia electoral deben contar con autonomía e independencia funcional, económica y técnica suficientes para garantizar este derecho.
 - b. Las autoridades responsables deben actuar de manera coordinada mediante protocolos claros de intercambio de información y remisión de casos, evitando vacíos de competencia.
2. Los partidos políticos, las agencias de publicidad y otros responsables o encargados de tratamiento deben registrar y contar con la evidencia del consentimiento libre, informado y específico de parte de los titulares para el uso de sus datos personales y datos personales sensibles ya sea por su adquisición directa o por su inferencia, previa información sobre cómo y a qué se destinan y cómo se procesarán sus datos.
3. Las autoridades deben reenfocar las prioridades y pasar de regular la moderación de contenidos a fortalecer e implementar las políticas de protección de datos personales, en particular los principios de finalidad, libertad, veracidad y acceso y circulación restringida:
 - a. Garantizar la prohibición del tratamiento de datos personales sensibles, incluyendo los inferidos, que revelen o puedan revelar la preferencia política de las personas.
 - b. En contextos electorales, el tratamiento de datos personales sensibles es sólo legítimo cuando se haya prestado consentimiento de forma previa, explícita y con propósitos de uso y transferencias estrictamente limitados y claramente informados.
 - c. El tratamiento debe realizarse solamente sobre los datos personales estrictamente necesarios para la finalidad que se persigue.
 - d. Prohibir sumar a usuarios a grupos de mensajería instantánea o listas de difusión con fines de divulgación política salvo en casos excepcionales en listas de miembros de partidos políticos o habiendo consentimiento previo e informado por parte del titular.
 - e. Garantizar la corresponsabilidad en el tratamiento de los datos personales de personas afiliadas a partidos políticos cuando estos contratan agencias de marketing o plataformas digitales para enviar publicidad dirigida a sus miembros.
 - f. Garantizar que partidos políticos y demás sujetos obligados cuenten con canales de comunicación fácilmente accesibles, a través de los cuales los titulares de los datos puedan ejercer sus derechos y solicitar información.

- g. Garantizar que la información sujeta a tratamiento sea veraz, completa, exacta, actualizada, comprobable, comprensible y que no induzca a error.

RECOMENDACIONES A EJECUTAR EN EL CORTO/ MEDIANO PLAZO

4. Crear mecanismos de cooperación, transparentes y accesibles para la ciudadanía, entre las autoridades de protección de datos, las autoridades electorales y/o las plataformas digitales para:
 - a. Construir canales fluidos de comunicación a través de, por ejemplo, acuerdos de colaboración formales a los fines de combatir la desinformación y el uso abusivo de datos personales de acuerdo a sus competencias.
 - b. Identificar y desarticular estrategias de desinformación coordinadas como granjas de bots, actividades online que simulan ser “orgánicos” de base ciudadana cuando en realidad están financiadas o coordinadas por un partido, gobierno o empresa, cuentas personales falsas manejadas por una entidad a los fines de manipular la opinión, entre otras.
 - c. Lograr tiempos de respuesta prioritarios para resolver denuncias en las plataformas sobre contenido que desinforma en tiempos electorales.
5. Las autoridades, partidos políticos, comunicadores y plataformas de redes sociales deberán garantizar en la medida de lo posible que la población tenga acceso a información relevante para la toma de decisiones electorales.
 - a. Los partidos políticos, autoridades electorales y autoridades de protección de datos deberán destinar un porcentaje de su presupuesto en comunicación para alertar de las consecuencias del microtargeting en contextos electorales.
 - b. Generar alianzas con los fact-checkers y otros comunicadores relevantes como organizaciones de la sociedad civil, influencers y otros, para identificar campañas de desinformación y comunicar a la población de las mismas por diferentes canales, incluyendo los oficiales del gobierno.
 - c. Sistematizar las propuestas electorales desarrolladas por los candidatos y sus plataformas electorales según ejes temáticos para facilitar la comparación entre partidos políticos.
 - d. Acordar estrategias entre autoridades y empresas de plataformas en línea, incluidas redes sociales y chatbots, a inicios de los periodos electorales para que se dé prioridad al contenido desarrollado por las autoridades electorales.
 - e. Promover el derecho de la ciudadanía a recibir información veraz, completa y objetiva sobre los procesos electorales. Esto incluye priorizar contenidos contrastados, contextualizados y de alta calidad informativa, facilitando que las personas identifiquen y eviten contenido falso, inexacto o manipulado.
 - f. Toda instancia, protocolo o política creada que involucre a autoridades o entes públicos debe ser comunicada siguiendo los estándares de la transparencia activa.

6. Las plataformas deberán inhabilitar herramientas de microtargeting para contenido político electoral durante periodos previamente establecidos.
7. Las autoridades, actores técnicos, académicos, sociedad civil y/o plataformas de redes sociales deberán colaborar en la creación de un laboratorio de análisis de impacto del uso de tecnologías digitales en contextos electorales que permita supervisar el cumplimiento de estas recomendaciones. Se analizará el impacto del uso de Inteligencia artificial generativa, la implementación de técnicas de microsegmentación y del despliegue de algoritmos de recomendación, entre otras. Específicamente se recomienda:
 - a. Elaborar informes sobre los resultados alcanzados en especial aquellos que den cuenta sobre la existencia de microtargeting, utilización de datos personales para segmentación, y la exposición a contenido variado en contextos electorales.
 - b. Establecer estrictos protocolos de ciberseguridad para los laboratorios que impidan el acceso a la información privada de las personas usuarias reales