Elecciones y Democracia
en la Era Digital

Una iniciativa de la Fundación Kofi Annan

LA PROTECCIÓN DE LA INTEGRIDAD ELECTORAL EN LA ERA DIGITAL

Informe de la Comisión
Kofi Annan sobre Elecciones
y Democracia en la Era Digital

Enero de 2020

ÍNDICE

Acerca de la Comisión Kofi Annan sobre Elecciones y Democracia en la Era Digital 1

Miembros de la Comisión 5

Prólogo 9

Resumen 14
El desarrollo de las capacidades propias 17
La creación de normas 18
La actuación de las autoridades públicas 20
La actuación de las plataformas 22

I. Las elecciones como elemento central de la lucha por la democracia 25

II. La polarización afectiva, las redes sociales y la integridad electoral 31
Las redes sociales y la polarización 35
Consecuencias para la acción 38

III. El discurso de odio y la integridad electoral 41
Enfoques para regular el discurso de odio 44
Consecuencias para la acción 49

IV. La protección de la integridad electoral contra la desinformación 55
La medición de la prevalencia de la desinformación 58
La instrumentalización de la desinformación 61
Consecuencias para la acción 62

V. La publicidad política en la era digital 71
Consecuencias para la acción 76

VI. La protección de las elecciones frente a la injerencia extranjera 81
Una industria transnacional emergente de manipulación electoral 83
La protección de la infraestructura electoral 84
Consecuencias para la acción 86

VII. Resumen de recomendaciones 91
El desarrollo de las capacidades propias 91
La creación de normas 93
La actuación de las autoridades públicas 94
La actuación de las plataformas 96

Agradecimientos 97

Acerca de la Fundación Kofi Annan 99

Bibliografía 101

LISTA DE FIGURAS

Recuadro 1 Las redes sociales como instrumento contra las mujeres 43

Recuadro 2 Las interrupciones del servicio de Internet en Asia y África 47

Recuadro 3 Iniciativas en favor de la diversidad en la codificación 52

Recuadro 4 El seguimiento ciudadano del discurso de odio en Kenya, 2012-2013 53

Recuadro 5 El enfoque de México para combatir la desinformación 66

Recuadro 6 El enfoque de Indonesia para combatir la desinformación, 2018-2019 68

Recuadro 7 El acuerdo de Abuja (Nigeria) sobre la conducta electoral, 2015 77

ACERCA DE LA COMISIÓN KOFI ANNAN SOBRE ELECCIONES Y DEMOCRACIA EN LA ERA DIGITAL

(KACEDDA)

A lo largo de toda su vida, Kofi Annan fue un defensor del derecho de todos los ciudadanos a incidir en cómo y quién gobierna. Insistió en que la gobernanza democrática y el empoderamiento ciudadano eran elementos integrales para el logro del desarrollo sostenible, la seguridad y la paz duradera; este principio guía gran parte del trabajo de la Fundación, especialmente su Iniciativa de Integridad Electoral.

En 2018, lanzó una de sus últimas grandes iniciativas; el señor Annan convocó a la integración de la Comisión sobre Elecciones y Democracia en la Era Digital. La Comisión incluye miembros de la sociedad civil y el gobierno, el sector tecnológico, el mundo académico y los medios de comunicación; quienes durante 12 meses examinaron y analizaron las oportunidades y los desafíos que afronta la integridad electoral como resultado de los avances tecnológicos.

> “La tecnología no se detiene, y tampoco debe hacerlo la democracia”.
>
> **- Kofi Annan**

Con la ayuda de un pequeño secretariado en la Universidad de Stanford, y la Fundación Kofi Annan, la Comisión llevó a cabo un proceso amplio de consultas y deliberaciones para estar en posibilidades de emitir recomendaciones sobre cómo las nuevas tecnologías, las plataformas de medios sociales y las herramientas de comunicación pueden utilizarse con el fin de involucrar, empoderar y educar a los votantes, así como fortalecer la integridad de las elecciones.

Preguntas clave que guiaron las deliberaciones de la Comisión:

- ¿Cuáles son los elementos fundamentales de la tecnología digital que tendrán un impacto exclusivamente negativo, o positivo, en la democracia y los procesos electorales?

- ¿Cuál es el potencial de las tecnologías digitales, tanto para fortalecer como para menoscabar la integridad del entorno electoral?

- ¿Cómo se puede emplear la tecnología en las elecciones, de forma transparente y responsable?

- ¿Qué oportunidades e incentivos puede ofrecer la tecnología digital a los votantes, especialmente a los jóvenes, para participar en procesos democráticos?

- ¿Qué función e impacto tiene el financiamiento político en el despliegue y uso de estrategias e instrumentos electorales, basados en la tecnología digital?

Objetivos de la Comisión:

1. Identificar y enmarcar los desafíos que afronta la integridad electoral, como resultado de la difusión a escala mundial de las tecnologías digitales y las plataformas de las redes sociales.

2. Adoptar medidas que atiendan estos desafíos y, a su vez, resalten las oportunidades que ofrece la innovación tecnológica para fortalecer la integridad electoral y la participación política.

3. Definir y articular un programa de promoción con miras a garantizar que los mensajes clave elaborados por la Comisión, se difundan y debatan ampliamente en todo el mundo.

Declaración de la Presidenta de la Comisión

"En esta era digital, las nuevas tecnologías y las plataformas de redes sociales están cambiando profundamente las democracias, y los procesos democráticos, en todo el mundo. Si bien brindan un potencial inigualable, a fin de cumplir las esperanzas de los ciudadanos de lograr una gobernanza democrática, también dan lugar a nuevos riesgos y dificultades para los procesos democráticos y los derechos políticos.

Junto con el equipo de Stanford y la Fundación Kofi Annan, mis homólogos comisionados y yo estamos decididos a honrar el legado del Sr. Annan y garantizar que esta Comisión desempeñe una función de liderazgo en la defensa y el fortalecimiento de los procesos electorales, que constituyen un elemento central de la democracia".

- Laura Chinchilla

PRESIDENTA DE LA COMISIÓN KOFI ANNAN SOBRE ELECCIONES Y DEMOCRACIA EN LA ERA DIGITAL

MIEMBROS DE LA COMISIÓN

La Comisión Kofi Annan sobre Elecciones y Democracia en la Era Digital reúne a algunos de los líderes más distinguidos del sector tecnológico, el mundo académico y la vida política, con el objeto de responder una sencilla pregunta: ¿Cómo podemos mitigar los riesgos que la era digital acarrea para nuestras elecciones, y al mismo tiempo, cómo aprovechamos esta oportunidad para fortalecer la democracia en todo el mundo?

Kofi Annan † - Presidente Convocante
(Ghana)

Premio Nobel de la Paz, Secretario General
de las Naciones Unidas de 1997 a 2007,
y Presidente Fundador de la Fundación Kofi Annan

Laura Chinchilla - Presidenta de la Comisión
(Costa Rica)

Vicepresidenta del Club de Madrid,
Ex-Presidenta de Costa Rica

Yves Leterme - Vicepresidente de la Comisión
(Bélgica)

Ex Secretario General IDEA Internacional
Ex Primer Ministro de Bélgica

Stephen Stedman - Secretario General de la Comisión
(Estados Unidos)

Investigador Senior del Instituto Freeman Spogli de Estudios Internacionales y profesor de Ciencias Políticas (Universidad de Stanford)

Noeleen Heyzer
(Singapur)

Ex Secretaria Ejecutiva de la Comisión Económica y Social para Asia y el Pacífico de las Naciones Unidas

Toomas Hendrik Ilves
(Estonia)

Miembro Visitante distinguido, Institución Hoover,
Ex Presidente de Estonia

Ory Okolloh

(Kenya)

Directora General de África en Luminate

Nate Persily

(Estados Unidos)

Titular de la Cátedra de Derecho James B. McClatchy en la Facultad de Derecho de la Universidad de Stanford

Alex Stamos

(Estados Unidos)

Profesor Investigador en la Universidad de Stanford, Ex Oficial Jefe de Seguridad de Facebook

William Sweeney

(Estados Unidos)

Ex Director General y Presidente de la Fundación Internacional para Sistemas Electorales (IFES)

Megan Smith

(Estados Unidos)

Fundadora y Directora General de Shift7, Ex Oficial Principal de Tecnología de los Estados Unidos

Ernesto Zedillo

(México)

Director del Centro de Estudios sibre la Globalización de la Universidad de Yale, Ex Presidente de México

PRÓLOGO

Actualmente la consolidación democrática afronta grandes desafíos en todo el mundo. La democracia se enfrenta a amenazas cada vez más insidiosas, especialmente debido a la manipulación de los procedimientos jurídicos y constitucionales originalmente diseñados para proteger acciones arbitrarias y abusos en contra de la democracia. El populismo y los movimientos de la posverdad ejercen una fuerte presión sobre las elecciones libres e imparciales, piedra angular de la legitimidad democrática, mediante el uso de las nuevas tecnologías y comunicaciones digitales, para confundir y engañar a la ciudadanía. En la actualidad, las elecciones libres e imparciales, principal expresión de la voluntad democrática que favorecen la gobernabilidad colectiva, están lejos de poder ser garantizadas en muchos países del mundo. Para protegerlas, es necesario un nuevo conjunto de políticas y acciones emprendidas por las plataformas tecnológicas, los gobiernos y la ciudadanía.

La vulnerabilidad de la integridad electoral en todo el mundo es un síntoma de procesos más amplios de deterioro democrático, perceptibles tanto en las democracias nuevas como en las más antiguas: el aumento de la polarización política, la disminución de la confianza, tanto entre los ciudadanos como entre la ciudadanía y las instituciones gubernamentales, los ataques sistemáticos contra la prensa y los medios de comunicación independientes, el declive de los partidos políticos como medios legítimos para sumar intereses, y la creciente frustración ante la imposibilidad de los gobiernos democráticos a la hora de satisfacer las necesidades y aspiraciones básicas de las personas.

El elemento central de estos cambios es el uso de las tecnologías digitales de la comunicación, que a menudo es considerado la fuente de este deterioro democrático. Algunos afirman que las redes sociales polarizan el debate público, pues hacen que las personas se posicionen en extremos políticos. Otros sostienen que las redes sociales crean "burbujas de filtro" y "cámaras de eco", de manera que se reduce el acceso a la variedad de fuentes de información y perspectivas que posibilitan la deliberación democrática. En vista de que las campañas políticas utilizan las redes sociales para dirigirse a pequeños grupos (*targets*) de votantes, con mensajes personalizados, hay quienes afirman que las redes sociales menoscaban la esfera pública y el proceso de negociación de las campañas electorales. En resumen, los debates actuales sobre las causas y los efectos del deterioro democrático, estarían incompletos si no se aborda y analiza la función real que las tecnologías de comunicación digital desempeñan en este proceso.

Por esta razón, Kofi Annan convocó la Comisión sobre Elecciones y Democracia en la Era Digital. Profundamente preocupado por los efectos que las tecnologías de la información y comunicación (TICs) estaban teniendo en la democracia y las elecciones: con base en conversaciones previas con expertos de todo el mundo, el Sr. Annan pensó que la creación de una nueva comisión podría arrojar luz sobre algunas de las cuestiones fundamentales relacionadas con las nuevas tecnologías de la información y la comunicación, las elecciones y la democracia. Es así como otorgó a la Comisión el mandato de identificar y enmarcar los desafíos que afronta la integridad electoral, como resultado de la difusión mundial de las tecnologías digitales y las plataformas de las redes sociales, así como desarrollar propuestas normativas para abordar estos retos.

El Sr. Annan pidió a la Comisión que aplicara un enfoque global y tratara de comprender estos problemas que se manifiestan en los distintos continentes, especialmente en las democracias del Sur Global. Con miras a ampliar su alcance, la Comisión realizó consultas con expertos y autoridades en el Brasil, México,

Kenya, Côte d'Ivoire, Sudáfrica y la India, y solicitó la elaboración de varios informes de investigación sobre América Latina, África y Asia. La Comisión también se reunió con la Comisión Europea y se puso en contacto con figuras destacadas de las industrias de Internet y las redes sociales.

En nuestro informe, la Comisión presenta una serie de recomendaciones encaminadas a fortalecer la capacidad de las autoridades en materia de integridad electoral, elaborar normas que adopten un enfoque compartido sobre el uso aceptable de las tecnologías digitales en las elecciones, y fomentar las capacidades de las autoridades públicas y las empresas del sector tecnológico, con objeto de fortalecer la integridad electoral. Estas recomendaciones se desprenden de una de las principales conclusiones del informe: todas las partes interesadas —plataformas tecnológicas y digitales, gobiernos, autoridades electorales, medios de comunicación tradicionales, y la ciudadanía— desempeñan un papel fundamental en el fortalecimiento de la integridad electoral.

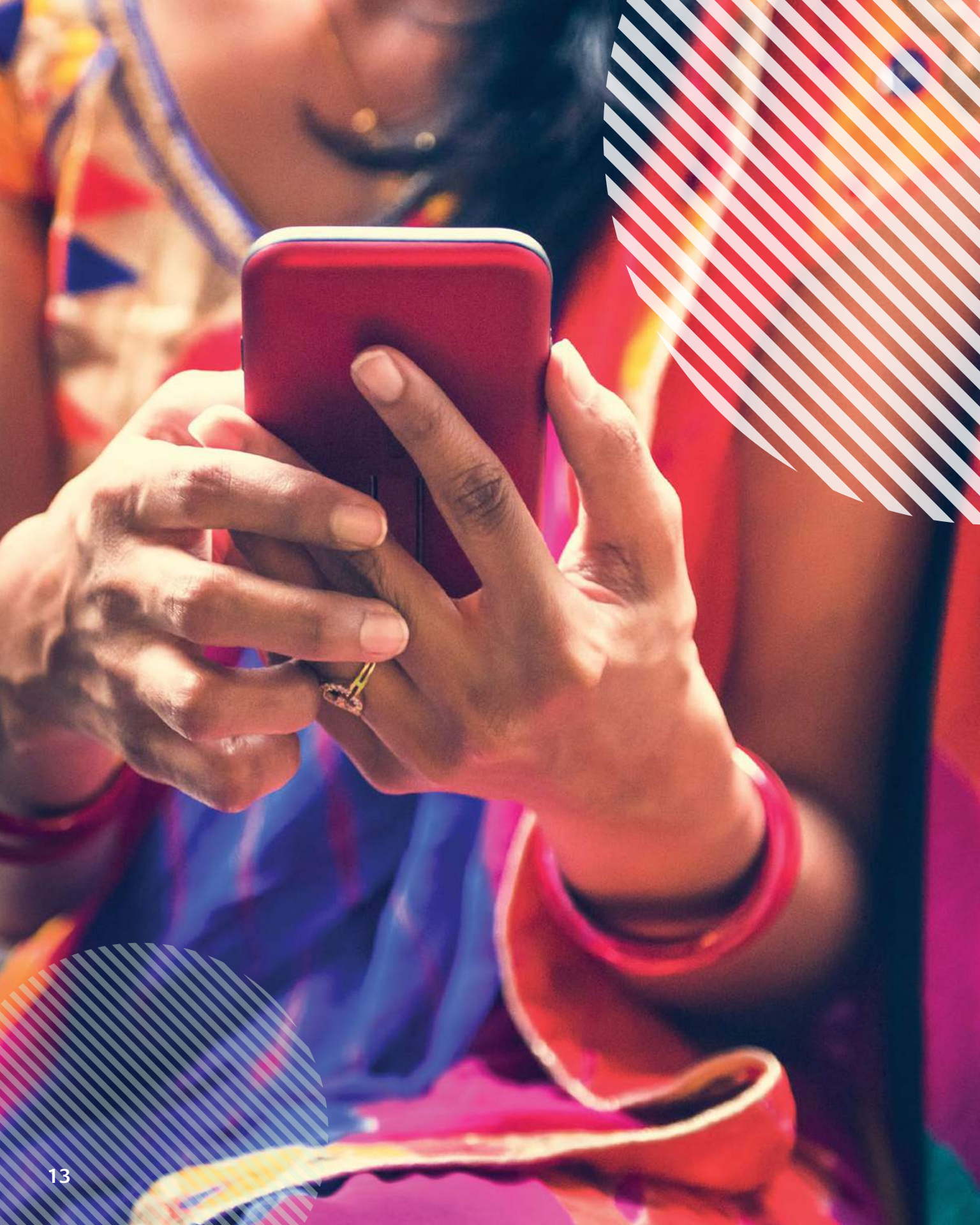
Me gustaría expresar mi gratitud a Yves Leterme, Vicepresidente de la Comisión, y mis colegas comisionadas y comisionados por su contribución y dedicación a este proyecto. En especial, quisiera expresar mi profundo agradecimiento al Secretario General de la Comisión, Stephen Stedman, por su trabajo en la supervisión de las investigaciones y consultas de la Comisión, y por su labor en la elaboración del informe. Asimismo, estoy muy agradecida por el apoyo recibido por parte de la Fundación Kofi Annan y su Presidente, Alan Doss, bajo cuyos auspicios fue convocada la Comisión.

El Sr. Annan falleció inesperadamente antes de que la Comisión comenzara su trabajo. Se interesó profundamente por las cuestiones relacionadas con la integridad electoral, sobre todo debido a su experiencia como mediador después de las fallidas elecciones de Kenya en 2007, cuando miles de ciudadanos perdieron la vida y cientos de miles más fueron desplazados por la fuerza, lo que estuvo cerca de desembocar en una guerra civil.

Por su visión, su defensa de la democracia y sus continuos esfuerzos para fortalecer el Estado de Derecho, y garantizar la paz internacional, dedicamos este informe a la memoria de Kofi. El legado de Kofi Annan como protector y defensor de la integridad electoral es verdaderamente significativo. Esperamos que este informe honre dicho legado y permita que perdure en las conversaciones y los debates futuros, pero sobre todo en las acciones encaminadas a fortalecer la integridad de las elecciones en todo el mundo.

- Laura Chinchilla

PRESIDENTA DE LA COMISIÓN KOFI ANNAN SOBRE ELECCIONES Y DEMOCRACIA EN LA ERA DIGITAL



RESUMEN

Las nuevas tecnologías de la información y la comunicación (TICs) plantean retos difíciles para la integridad electoral. En los últimos años, los gobiernos extranjeros han utilizado las redes sociales e Internet para interferir en las elecciones a escala mundial. La desinformación se ha utilizado como herramienta para desacreditar a las instituciones democráticas, sembrar la desconfianza social y atacar a las candidaturas políticas. Las redes sociales han demostrado ser una herramienta útil para que los grupos extremistas envíen mensajes de odio e inciten a la violencia. Los gobiernos democráticos se esfuerzan por hacer frente a una revolución en la publicidad política, causada por las tecnologías de la información y la comunicación. La integridad electoral se ha visto amenazada por los ataques en contra de los procesos electorales y de la calidad de la deliberación democrática.

La relación entre Internet, las redes sociales, las elecciones y la democracia es compleja, sistémica y está en ciernes. Nuestra capacidad para evaluar algunas de las afirmaciones más importantes sobre las redes sociales se ve limitada por la falta de voluntad de las principales plataformas a la hora de compartir datos con los investigadores. No obstante, confiamos en algunos hallazgos de gran importancia:

- Muchos de los males de los que se acusa a Internet y a las redes sociales —la extrema polarización de la política democrática; la disminución de la confianza en los gobiernos, los medios tradicionales y la ciudadanía; los medios partidistas y la difusión de la desinformación— son anteriores al auge de las redes sociales e Internet.

- Si bien las redes sociales no son una causa de polarización política a gran escala, la exacerban e intensifican, y constituyen una herramienta a disposición de cualquier persona que pretenda socavar la integridad electoral y la salud de la deliberación democrática.

- Las democracias varían en cuanto a su vulnerabilidad frente a la desinformación, en función de la polarización, la desconfianza y los medios tradicionales partidistas preexistentes; las nuevas democracias y regímenes en transición en el Sur Global son especialmente vulnerables.

- En un futuro previsible, las elecciones en las democracias del Sur Global constituirán el elemento central en la red del discurso de odio, la desinformación, la injerencia externa y la manipulación nacional.

- La responsabilidad ante el abuso de las redes sociales como amenaza a la integridad electoral recae sobre múltiples agentes:

    - Las grandes plataformas permitieron que el discurso de odio y la desinformación se volvieran virales; no pudieron anticipar el uso que se haría de sus tecnologías en las democracias de transición, con sociedades fracturadas e historiales de violencia étnica y religiosa; negaron la evidencia de que sus productos menoscababan la democracia y fomentaban la violencia; participaron en campañas de desprestigio contra los detractores, y tardaron demasiado en reaccionar de manera constructiva.

    - Las personas candidatas y electas han utilizado las redes sociales para fomentar el odio, difundir la desinformación y menoscabar la confianza en las instituciones sociales y gubernamentales.

- Algunas consultorías políticas han tratado de manipular los procesos electorales con el fin de ganar a toda costa, y han convertido la manipulación electoral en un negocio transnacional que amenaza la integridad electoral en todo el mundo.

- Los medios de comunicación tradicionales a menudo han aumentado la desinformación y la propaganda, en lugar de desenmascararla.

La defensa de la integridad electoral contra el uso indebido y el abuso de las redes sociales dependerá de las decisiones y el comportamiento de las principales empresas y plataformas tecnológicas, así como de los gobiernos, las y los políticos, los medios tradicionales, los órganos electorales y la ciudadanía. Con el fin de proteger la integridad electoral en la era digital, necesitaremos fortalecer las capacidades de quien defiende dicha integridad y elaborar normas compartidas sobre el uso adecuado de las tecnologías digitales en las elecciones. Las plataformas tecnológicas y las autoridades públicas deben adoptar medidas encaminadas a reforzar la integridad electoral.

EL DESARROLLO DE CAPACIDADES PROPIAS

Recomendación núm. 1.

Se debe prestar más atención y destinar más recursos a la promoción de la integridad electoral. Las autoridades públicas, las organizaciones internacionales, las fundaciones filantrópicas y la sociedad civil deben invertir en el desarrollo de habilidades tecnológicas y capacidad digital, en los esfuerzos mediáticos y en los órganos electorales que protegen y promueven la integridad electoral.

Todas las partes interesadas deben cooperar, colaborar y compartir con rapidez la información relacionada con las amenazas a la integridad electoral. Estas actuaciones deben incluir:

- La creación de un índice de vulnerabilidad electoral que mida qué elecciones requieren un seguimiento estricto de las posibles injerencias electorales, el comportamiento falaz coordinado en línea, y la desinformación posibles.
- El desarrollo de capacidades porpias de las asociaciones nacionales cuyo objetivo consiste en defender la integridad de las elecciones, frente a la instrumentalización de la desinformación, así como apoyar la mejora de las prácticas de evaluación e intercambio de información.
- La financiación de las organizaciones de la sociedad civil que luchan contra el discurso de odio, el acoso selectivo y la incitación a la violencia, especialmente en el período previo a las elecciones.
- La ayuda dirigida a los órganos electorales, con miras a adquirir conocimientos especializados relativos a las mejores prácticas de ciberseguridad.
- El apoyo a las democracias para desarrollar programas de tecnología cívica a través de la formación en codificación, especialmente para las mujeres y las minorías, y mediante la incorporación de personal con habilidades técnicas en los equipos gubernamentales.

Recomendación núm. 2.

Algunos órganos electorales pueden necesitar asistencia técnica a corto plazo para hacer frente a las amenazas a la integridad electoral causadas por la injerencia extranjera en las elecciones, la piratería y los discursos de odio, que conducen a la violencia relacionada con las elecciones. En tales casos, la asistencia técnica internacional para apoyar a estos órganos a defender su proceso electoral debe estar disponible en el momento en que se solicite. Con el fin de garantizar que dicha asistencia se brinde con apremio, se recomienda el desarrollo de equipos permanentes de ciberseguridad electoral que puedan desplegarse inmediatamente bajo petición. Dichos equipos podrían formar parte de organizaciones internacionales existentes, como la División de Asistencia Electoral de las Naciones Unidas, organizaciones regionales, o una nueva institución internacional. Asimismo, deben poder emplear turnos rotativos en la ocupación de puestos técnicos, a fin de garantizar la aplicación de las mejores prácticas gubernamentales en el plano digital.

LA CREACIÓN DE NORMAS

Recomendación núm. 3.

Refrendamos el llamado que hace la Comisión Transatlántica sobre la Integridad de las Elecciones a que las personas candidatas, partidos y grupos políticos firmen compromisos de rechazo de las prácticas engañosas de campaña digital. Dichas prácticas incluyen el uso de datos o materiales robados, la utilización de imágenes manipuladas —como la manipulación de imágenes, vídeos y audios; la creación de éstos empleando la inteligencia artificial; y la difusión de desnudos generados digitalmente—, la producción, uso o difusión de materiales falsificados, y la confabulación con gobiernos extranjeros y sus agentes que tratan de manipular las elecciones.

Recomendación núm. 4.

Los gobiernos democráticos deben ponerse de acuerdo y aprobar una convención internacional sobre el papel de los gobiernos extranjeros y sus agentes en las elecciones de otros países. En especial, deben desarrollar normas internacionales que distingan la asistencia transfronteriza legítima de las intervenciones ilícitas o ilegales.

Recomendación núm. 5.

Los gobiernos democráticos deben considerar las tecnologías electorales electrónicas como infraestructura vital, y apoyar la norma refrendada por el Grupo de los 20, conforme a la cual los "Estado[s] no deben llevar a cabo ni apoyar conscientemente actividades en materia de tecnología de la información y las comunicaciones [...] que dañen intencionalmente la infraestructura vital".

Recomendación núm. 6.

Los proveedores de equipos y servicios electorales deben comprometerse a cumplir un código de conducta con el fin de garantizar que sus productos sean seguros y sus prácticas comerciales protejan los derechos, la privacidad y los datos de los ciudadanos en sus países clientes, así como adoptar prácticas de adquisición honestas y transparentes. A su vez, la comunidad internacional del sector de la integridad electoral se debe comprometer a condicionar la asistencia electoral a los países, a la firma y cumplimiento del código por parte de los proveedores. Una iniciativa de múltiples partes interesadas, en la que participe, como mínimo, la comunidad de la integridad electoral, la Red Global de Monitores Electorales Nacionales y los asociados internacionales, quienes deberán elaborar dicho código de conducta.

Recomendación núm. 7.

La comunidad que trabaja en el ámbito de la integridad electoral debe crear normas y estándares para los consultores de campañas políticas transnacionales, incluidas las empresas de relaciones públicas y comunicaciones estratégicas, y los comercializadores digitales. La regulación gubernamental debe desarrollar procedimientos para la certificación de estos consultores, a fin de impedir que una empresa que infrinja las normas, reglas y estándares relativos a la consultoría de campañas continúe trabajando en procesos electorales.

LA ACTUACIÓN DE LAS AUTORIDADES PÚBLICAS

Recomendación núm. 8.

Los países deben adaptar su reglamento de publicidad política al entorno en línea. Las autoridades públicas competentes deben:

- Definir por vía legislativa qué se considera un anuncio político.
- Obligar a las plataformas de redes sociales a publicar toda la información relacionada con la adquisición de un anuncio, incluida la identidad real del anunciante, la suma pagada, el criterio de segmentación, y el verdadero trabajo creativo del anuncio.
- Especificar en la legislación el tamaño mínimo del segmento de público para un anuncio.
- Establecer jurídicamente un período de reflexión mínimo para los anuncios políticos digitales, de 48 horas previas a las elecciones.

Recomendación núm. 9.

Las autoridades públicas deben obligar a las principales plataformas de Internet a proporcionar a las partes independientes datos significativos sobre el impacto que las redes sociales tienen en la democracia. En concreto, las plataformas deben:

- Compartir datos seguros que protejan la privacidad, con instituciones académicas certificadas, para el estudio de cuestiones como el análisis de algoritmos en materia de tendencias extremistas, la comprensión del efecto de las redes sociales en la polarización política y el consumo de información, y el esclarecimiento de la relación entre el discurso de odio en línea y la violencia física.

- Actualizar los informes de transparencia con miras a hacer públicos los datos relativos al número de denuncias de discurso de odio y abusos en línea; se deben incluir datos sobre los casos de abuso selectivo (por razón de género, raza, orientación sexual o religión) y la frecuencia con la que distintas comunidades se ven afectadas.

- Identificar las cuentas automatizadas; cuando las plataformas no identifiquen correctamente las cuentas automatizadas (p. ej., un bot), se les deben imponer sanciones económicas.

Recomendación núm. 10.

Las autoridades públicas deben promover los programas de alfabetización digital y mediática en las escuelas, así como la programación de interés público entre la población general.

LA ACTUACIÓN DE LAS PLATAFORMAS

Recomendación núm. 11.

Las plataformas deben ofrecer mayor transparencia en lo relativo a los anuncios políticos:

- Las plataformas deben ofrecer a los usuarios la opción de incluir o excluir la publicidad política.

- Las plataformas solo deben permitir la adquisición de anuncios a aquellas personas candidatas, partidos y grupos que se hayan comprometido a evitar las prácticas de campaña engañosas. Posteriormente, tales compromisos deben convertirse en las normas de funcionamiento de las plataformas para decidir si aceptan un anuncio dado.

- A fin de evitar el encubrimiento de las fuentes de financiación tras etiquetas organizacionales engañosas, las plataformas deben requerir que se publique la identidad de las personas que financian los anuncios políticos.

Recomendación núm. 12.

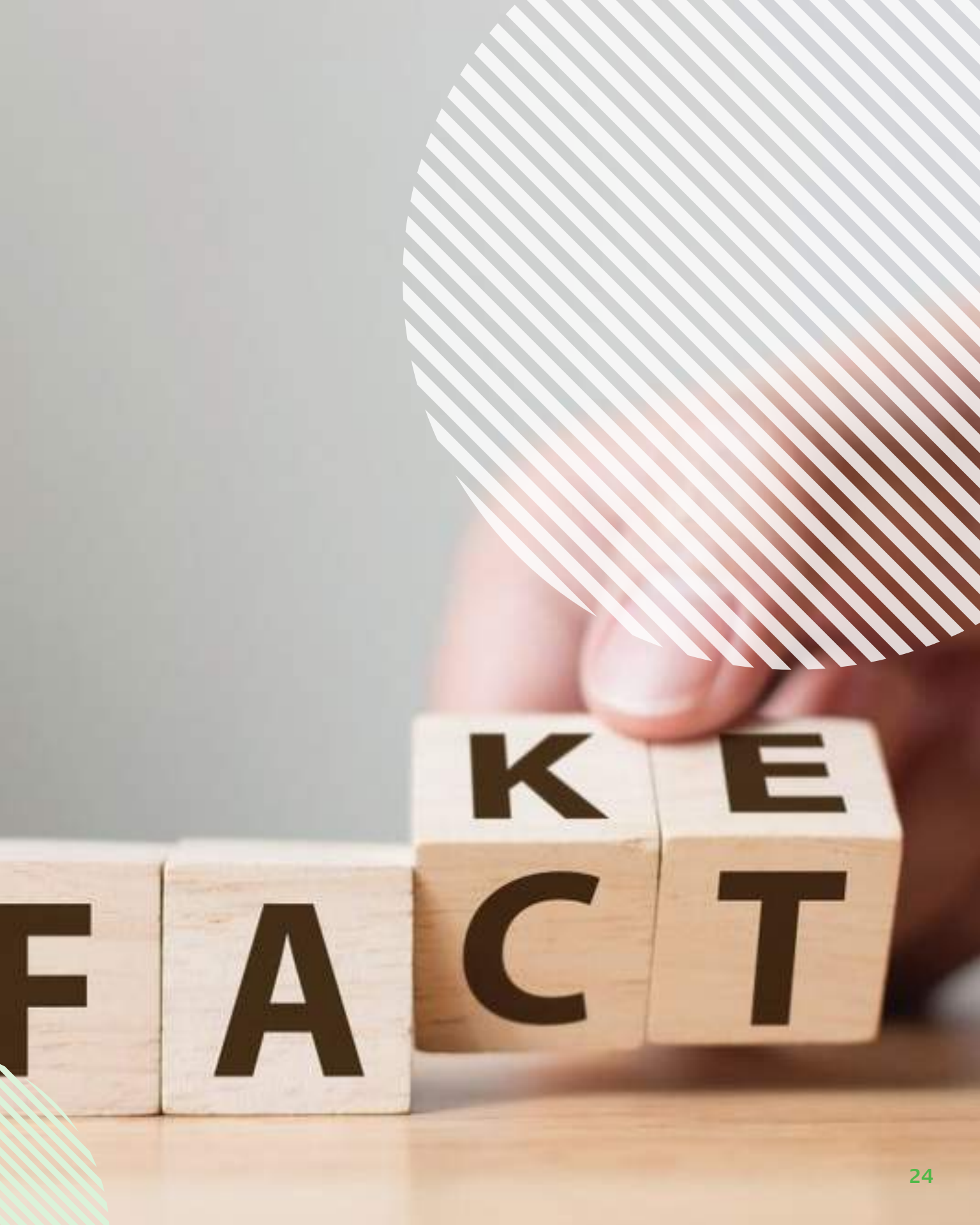
Las plataformas de redes sociales deben desarrollar sistemas de alerta temprana con miras a detectar la desinformación electoral, la injerencia extranjera, los crímenes de odio, las amenazas contra las mujeres, la violencia y la supresión de los votantes:

- Deben emplear más expertos que dominen los idiomas locales y que tengan competencia cultural en el lugar en donde operan.

- Toda vez que cuando la comunicación ya se ha hecho viral es demasiado tarde para tomar medidas, los sistemas de alerta temprana deben comenzar a aplicar la revisión por parte de personas físicas, de las cuentas y las publicaciones que representan una posible amenaza para las elecciones. Una persona física ha de encargarse de la revisión y del control del contenido que, en mayor o menor medida, se hace viral.

Recomendación núm. 13.

Las plataformas de redes sociales deben crear una coalición con el propósito de afrontar las amenazas digitales a la democracia y a la integridad de los procesos electorales, de manera similar a la colaboración mantenida en el ámbito de la lucha contra el terrorismo y la explotación infantil. Los miembros de las coaliciones deben reunirse con regularidad y crear estrategias para múltiples plataformas, a fin de detectar y limitar el alcance de la instrumentalización de la desinformación.


FAKE
FACT

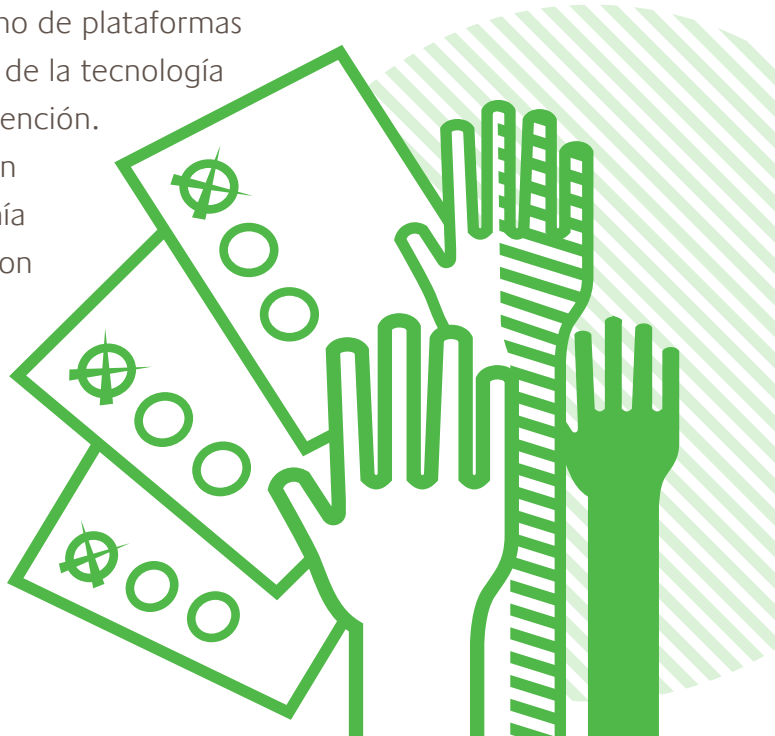
I. LAS ELECCIONES COMO ELEMENTO CENTRAL DE LA LUCHA POR LA DEMOCRACIA

Las tecnologías de comunicaciones digitales han hecho que aquellos que explotan las fisuras de la democracia moderna puedan menoscabar las elecciones y la deliberación democrática. Los partidos, personas candidatas, consultorías de campaña y gobiernos extranjeros han instrumentalizado las redes sociales con miras a difundir desinformación, incitar al odio y la violencia, e interferir en las elecciones, tanto nacionales como extranjeras. En un entorno global caracterizado por el incremento de la polarización y los niveles de desconfianza, las elecciones están al frente de la lucha por la democracia.

Las propiedades excepcionales de las nuevas tecnologías de la información y las comunicaciones (viralidad, velocidad, anonimato, homofilia y alcance transnacional) crean nuevos desafíos para la democracia que afectan al mundo entero[1]. Antes de que lo ocurrido en las elecciones presidenciales de los Estados Unidos en 2016 acaparara el debate público, en las que los bots políticos y troles rusos alimentaron la desinformación, con el fin de sembrar la desconfianza social y debilitar a las candidaturas, ya se habían desarrollado, refinado y utilizado las mismas estrategias en Kenya, Filipinas y Nigeria, entre otros países. Algunas empresas de consultoría sin escrúpulos, como Cambridge Analytica, emplearon tácticas de guerra de la información durante elecciones en África, Asia y América Latina, varios años antes de su campaña en los Estados Unidos y el Reino Unido. Asimismo, los partidos políticos y candidaturas populistas han explotado las redes sociales con el fin de alimentar el sentimiento nacionalista, difundiendo el odio y la intolerancia, con miras a incorporar sus alternativas agendas en los debates generales.

Sin embargo, las investigaciones realizadas hasta la fecha indican que los efectos de estas tecnologías no son homogéneos ni negativos en todos los casos. Sin duda, las tecnologías digitales pueden exacerbar la agitación política en países en los que ya existe cierta polarización y desconfianza. Como concluye nuestro informe sobre las redes sociales y la democracia en América Latina, los efectos de las redes sociales "amplían patrones previos en lugar de crear nuevos"[2]. Los estudios en África y América Latina también concluyeron que existen efectos positivos graduales en la participación política, como el aumento de la participación electoral, la adhesión a movimientos sociales y la coordinación de la acción política[3]. En África, las plataformas digitales son catalizadores significativos que permiten la difusión de los movimientos sociales y constituyen un medio importante, incluso fundamental, para el diálogo político, el intercambio de información y la deliberación democrática[4].

A medida que las redes sociales ganan relevancia en la política del siglo XXI, tanto en materia de herramientas de campaña como de plataformas en favor de la deliberación pública, el efecto de la tecnología en la integridad electoral exige una mayor atención. De hecho, las tecnologías digitales repercuten directamente en la forma en que la ciudadanía participa en la democracia, y las elecciones son períodos críticos en los que la ciudadanía presta una gran atención al discurso público. Las elecciones son pruebas únicas de legitimidad democrática, y las percepciones de su integridad pueden tener grandes efectos sobre la estabilidad y el desempeño democráticos.



Nuestro mandato consiste en identificar los desafíos que las nuevas tecnologías de la información y las comunicaciones plantean para la integridad electoral, y desarrollar medidas normativas que destaquen las oportunidades proporcionadas por las tecnologías digitales, para fortalecer la integridad electoral y mitigar los daños causados por la innovación tecnológica. La integridad electoral se define como "cualquier elección basada en los principios democráticos de sufragio universal e igualdad política, reflejados en acuerdos y normas internacionales, cuya preparación y administración es profesional, imparcial y transparente, a lo largo de todo el ciclo electoral"[6]. Nos centramos no solo en cómo las redes sociales pueden afectar al desarrollo de unas elecciones, sino también en el efecto que pueden tener en las *percepciones sobre la integridad de éstas*. Tal y como advierte una organización no gubernamental (ONG), "si los votantes y los candidatos creen que una elección es fraudulenta o ha sido mal administrada, es posible que no acepten el resultado. En el mejor de los casos, esto puede generar descontento o desinterés público; en el peor, violencia, gobernanza ineficaz e inestabilidad a largo plazo"[6].

Un componente de la integridad electoral al que prestamos especial atención, es el entorno en el que tienen lugar las elecciones y si los participantes (candidaturas, partidos y simpatizantes) confían en su seguridad mutua[7]. La integridad electoral requiere que la ciudadanía crea que las elecciones son un juego que se repite y seguirá celebrándose en el futuro. En muchas democracias de transición, los contendientes políticos temen que si pierden unas elecciones quedarán excluidos del poder de forma permanente. Las personas candidatas, partidos y simpatizantes deben estar seguros de que si pierden unas elecciones tendrán la oportunidad de organizarse y participar en elecciones futuras, y de que quien gane no utilizará su poder para inhabilitarles. También deben confiar en que si ganan unas elecciones, obtendrán la capacidad de formar un gobierno y seguir su agenda normativa, y en que quienes pierdan no recurrirán a la violencia ni bloquearán su mandato electoral.

Las tecnologías de la información y las comunicaciones, especialmente las redes sociales, plantean varios desafíos potenciales para la integridad electoral, y en nuestro informe abordamos todos y cada uno de ellos: la polarización, el discurso de odio, la desinformación, las nuevas formas de publicidad política y la injerencia extranjera. Si bien nos centramos en los desafíos específicos que las tecnologías de la información y las comunicaciones plantean para la integridad electoral, en las diferentes consultas que realizamos en todo el mundo se expresaron dos preocupaciones de gran importancia relacionadas con la gobernabilidad democrática.

En primer lugar, personas legisladoras, desde Europa hasta América Latina, expresaron su convencimiento de que la velocidad y la omnipresencia de las redes sociales generan presión para responder con inmediatez a las demandas, las noticias, las reclamaciones y las acusaciones; y menoscaban el mandato de los parlamentos para deliberar y establecer agendas normativas. Algunos parlamentarios consideraron que la naturaleza misma de la representación política se estaba desmoronando debido a la intensa movilización de la opinión en línea y la capacidad de las campañas en las redes sociales para imponer un estricto escrutinio de la vida cotidiana de los cargos electos. En algunos países, la toxicidad de los ataques y las amenazas personales en línea han hecho que personas parlamentarias, en su gran mayoría mujeres, abandonen la vida política. Si bien los efectos de las redes sociales en la calidad de la gobernanza democrática superan los límites de nuestro mandato, consideramos que es una cuestión que merece un mayor escrutinio e investigación.

En segundo lugar, escuchamos en repetidas ocasiones la preocupación relativa a la posibilidad de supervivencia de la democracia en un mundo en donde no hay control sobre las noticias falsas y la ciudadanía no pueden ponerse de acuerdo sobre hechos básicos. Si bien la calidad de la deliberación democrática puede haber empeorado en algunas de las democracias más antiguas, cabe

señalar que las críticas actuales sobre la pobreza de la deliberación en nuestra democracia son anteriores al auge de Internet[8]. Así como las noticias falsas y el discurso de odio existen desde hace siglos, la ciudadanía de las democracias en su conjunto nunca ha compartido los mismos hechos o se ha puesto de acuerdo en qué constituye un hecho. A menudo ésta no está de acuerdo sobre los hechos fundamentales y, sin duda, no vota sobre la base de verdades compartidas[9]. La democracia es necesaria precisamente porque la ciudadanía no está de acuerdo sobre los hechos de facto. Incluso en la era digital, la democracia ofrece varias ventajas que el autoritarismo no permite: una mayor protección de los derechos y las libertades, una mejora en el acceso a la información, un aumento de las oportunidades de interacción entre la ciudadanía, y una mayor probabilidad de que el debate sea significativo.

Como propuesta normativa, coincidimos en que la calidad de la democracia mejora cuando la ciudadanía tiene una misma visión sobre los hechos y lo que constituye un hecho, y en que debemos esforzarnos por mejorar la deliberación democrática.

II. LA POLARIZACIÓN AFECTIVA, LAS REDES SOCIALES Y LA INTEGRIDAD ELECTORAL

La polarización plantea cada vez más desafíos a la gobernabilidad, la cohesión social y la democracia. La polarización tiene múltiples facetas; no obstante, este informe se centra especialmente en la polarización afectiva, en la que el ánimo partidista lleva a los seguidores políticos a sostener opiniones y creencias negativas sobre sus oponentes. Cuando la polarización afectiva se agrava, "las personas perciben y describen cada vez más la política y la sociedad en términos de 'nosotros' contra 'ellos'"[10], lo que conlleva posibles efectos tóxicos para la integridad electoral. Tal y como establece un informe anual sobre la democracia, "una vez que las élites políticas y sus seguidores dejan de creer que los opositores políticos son legítimos y merecen el mismo respeto, o incluso son aceptables como familiares y amigos, es menos probable que se adhieran a las normas democráticas en la lucha por el poder"[11].

En los Estados Unidos, la polarización ha aumentado de manera constante desde la década de 1970[12]. Antes de la difusión de Internet, la aparición de los teléfonos inteligentes y el auge de las redes sociales, la polarización política era avivada por los medios de comunicación tradicionales partidistas[13]. El nacimiento de las noticias por cable en la década de 1980, el fin del principio de imparcialidad en 1987, y la aparición de la radio del odio, dieron lugar a un ecosistema de medios de comunicación extremamente partidistas en los Estados Unidos, que presentaba una gran desconfianza hacia los medios tradicionales y era vulnerable a las teorías de conspiración y propaganda[14]. Este ecosistema se ha convertido en un foro para los peores excesos de la desinformación y la incitación al odio de Internet y es una plataforma para personas políticas, expertas y periodistas irresponsables[15].

El ejemplo de Estados Unidos sugiere que los países en los que ya existen la polarización, la desconfianza en los medios de comunicación tradicionales y los ecosistemas mediáticos partidistas son mucho más vulnerables a las manipulaciones

de las redes sociales que los países con baja polarización y desconfianza[16]. Allí donde la polarización ya es elevada, las redes sociales pueden convertirse fácilmente en herramientas para exacerbar e intensificar la división política y el conflicto. En aquellos en los que la confianza en los medios tradicionales es baja, la ciudadanía evita las noticias objetivas. Los medios de comunicación claramente partidistas apelan a los peores instintos de sus lectores. Por consiguiente, es necesario ser precavido a la hora de generalizar los efectos de las redes sociales en países con instituciones, divisiones sociales y ecosistemas mediáticos muy variados.

De alguna manera, los Estados Unidos son un caso extremo entre las democracias antiguas en cuanto a su grado de polarización, medios de comunicación partidistas y desconfianza[17]. En un estudio reciente que mide la polarización afectiva en función de si "el debate público es respetuoso, objetivo y los opositores están abiertos a la persuasión a través de la razón", Estados Unidos ocupa el puesto 98 de un total de 178 países y se posiciona más cerca de la India (102), Polonia (109), el Brasil (117), y Hungría (127), que de democracias antiguas como Noruega (1), Suiza (2) o Dinamarca (3)[18].

Las democracias en el resto del mundo muestran un panorama variado. Muchas democracias en Asia, América Latina y África se encuentran entre las primeras en términos de polarización afectiva; sin embargo, algunos de los incrementos más significativos se han producido en Europa Occidental.

Los estudios empíricos indican que cuando existe polarización y desconfianza en los países de forma general, estos no son elementos nuevos, sino producto de tendencias a largo plazo anteriores al auge de las redes sociales[19].

Si bien la polarización política ha aumentado en algunas democracias, la confianza entre la ciudadanía hacia los medios de comunicación y hacia los parlamentos o las legislaturas suele estar en declive[20]. En la mayoría de los países, se ha registrado un descenso continuado de la confianza entre ciudadanos. Además, se observa una disminución gradual en el porcentaje de personas que expresan una "gran confianza" en los medios de comunicación en Europa, América Central, América del Sur y América del Norte. África muestra el declive general más significativo y la mayor inestabilidad; Asia y Oceanía es la única región que ha registrado un aumento neto de la confianza en la prensa durante las últimas tres décadas.

La confianza ciudadana en el parlamento ha disminuido, pero lo ha hecho de manera más variable. En América del Norte, Europa, América Central, América del Sur y África, se ha registrado una reducción en el porcentaje de personas que manifiestan una "gran confianza" en su legislatura en los últimos treinta años. La única región atípica ha sido Asia y Oceanía, que mostró un ligero aumento general desde principios de la década de 1980 hasta el período de la encuesta comprendido entre 2010 y 2014. La pérdida de confianza gradual no se debe tanto a los comportamientos generacionales, sino a los juicios de la ciudadanía sobre las acciones del gobierno y su fiabilidad, lo que sugiere que cuando las democracias cumplen sus objetivos, los ciudadanos responden positivamente[21]. El aumento de la polarización política y la disminución de la confianza amenazan la integridad electoral. La polarización política y la desconfianza debilitan la creencia en la seguridad mutua y, una vez esta comienza a deteriorarse, la desinformación en línea organizada y el discurso de odio pueden contaminar los entornos electorales.

El miedo puede apoderarse de los votantes que creen que si su partido pierde a corto plazo, lo hará para siempre. Las elecciones se centran únicamente en ganar, con poca consideración por las reglas, las leyes, la ética o las normas democráticas.

Muchas democracias de transición en el Sur Global muestran una polarización elevada, poca confianza y unos medios partidistas; por tanto, son altamente vulnerables a la desinformación en línea y al discurso de odio. Las elecciones en estos países son actualmente el elemento central de la violencia y la desestabilización, y las redes sociales se utilizan como instrumentos para intensificar la polarización y debilitar las normas de seguridad mutua necesarias para garantizar la integridad electoral. Esta tendencia no solo continuará, sino que es probable que aumente.

La conclusión de que los países con alta polarización son más vulnerables a la instrumentalización de los medios sociales no exime en ningún modo a las plataformas de responsabilizarse por los efectos nocivos de sus productos. Estas se apresuraron en llevar sus productos a países como Myanmar, Sri Lanka y Kenya, extremadamente vulnerables a la desinformación, la propaganda y el discurso de odio. Las plataformas no tuvieron en cuenta el modo en que se utilizarían sus productos en países sumamente polarizados con episodios de violencia. Una vez se dieron cuenta de su potencial mortífero, tardaron demasiado en subsanar el problema.

Las causas de la polarización a largo plazo son complejas y tienen múltiples facetas. Cada vez hay más estudios que señalan el aumento constante de la desigualdad económica como causa de la polarización[22] y del incremento del apoyo a posiciones políticas más extremas[23].

Otra investigación sugiere que los sistemas electorales gozan de gran importancia y que las democracias con un sistema de mayoría relativa son más propensas a la polarización extrema[24]. Otras apuntan a las crecientes preocupaciones sobre el estado de los residentes y personas trabajadoras rurales, que se sienten abandonadas por el dinamismo y el crecimiento urbanos y amenazados por la inmigración[25]. Del análisis de estas causas se desprenden varias posibles recomendaciones, a saber: aplicar políticas sociales y económicas que protejan a la clase media y la mano de obra[26], introducir reformas políticas que mitiguen los resultados y las percepciones de suma cero[27], y crear oportunidades sociales para que los distintos grupos interactúen, deliberen de forma conjunta y forjen un compromiso con identidades políticas más amplias[28]. Sugerir recomendaciones sobre cómo las sociedades pueden prevenir mejor la polarización extrema supera el alcance de esta Comisión; sin embargo, para nosotros está claro que constituye una primera línea defensiva fundamental para el desarrollo de la inmunidad a las distorsiones de las redes sociales.

LAS REDES SOCIALES Y LA POLARIZACIÓN

La importancia de Internet y las redes sociales como plataformas para el consumo de noticias e información ha generado crecientes preocupaciones sobre las formas en que la tecnología podría exacerbar o agravar la polarización. Desde los comienzos de Internet, algunos académicos plantearon que las redes sociales propician la aparición de burbujas de filtro y cámaras de eco, y segregan a las personas en grupos que leen las mismas noticias, se comunican solo entre sí y,

por lo tanto, piensan igual, lo que ejerce un efecto nocivo sobre el modo de gobernanza de las democracias[29]. El filtrado algorítmico, individual y social del contenido repercute en los tipos de información a los que están expuestos las personas. Los detractores sugieren que votantes que pasan tiempo en línea pueden no acceder a una selección representativa, equilibrada o precisa de las noticias y la información, y que la difusión de la información de calidad puede no distribuirse por igual entre el total de la población con derecho a voto. Del mismo modo, algunos periodistas argumentan que los algoritmos radicalizan porcentajes significativos de la población al proporcionar contenido que lleva a las personas a adoptar posiciones más extremas. La cobertura mediática reciente sugiere que existen sesgos en los algoritmos de las redes sociales que proporcionan contenidos extremistas a usuarios, como el motor de búsqueda de Google, que posiciona antes las páginas web que niegan el holocausto que las fuentes legítimas de información[30], o la función de reproducción automática de YouTube, que recomienda a los usuarios contenidos cada vez más radicales[31].

Sin embargo, las investigaciones a este respecto no han sido concluyentes por dos razones. En primer lugar, es difícil distinguir entre personas usuarias que tienden a asociarse voluntariamente con personas y fuentes de noticias que refuerzan su opinión política y su visión del mundo, y quienes siguen contenido que no elegirían por sí mismos pero que proporciona un algoritmo a través de otras fuentes y recomendaciones. En segundo lugar, las plataformas no han facilitado los datos necesarios para que los investigadores puedan responder la pregunta.

Las investigaciones sugieren que las redes sociales promueven en realidad la diversidad mediática y el acceso a una variedad de puntos de vista políticos y fuentes de información, especialmente en comparación con las fuentes de noticias tradicionales[32]. Del mismo modo, las plataformas facilitan las interacciones transversales conectando a las personas con sus familiares

y amistades cercanas, así como con parientes, colegas de trabajo o personas conocidas —relaciones que podríamos considerar “lazos débiles”—, que tienen más probabilidades de publicar o compartir contenido ideológicamente diverso[33]. Esta dinámica posibilita que las plataformas de redes sociales amplíen la variedad de puntos de vista políticos a los que están expuestas las personas usuarias.

Al mismo tiempo, puede que algunas personas vivan en cámaras de eco y otras no.

Las investigaciones en Alemania, España y los Estados Unidos muestran que los usuarios de Twitter dentro de redes heterogéneas suelen crear redes más moderadas desde un punto de vista político a lo largo del tiempo, lo que sugiere que quienes ya están predispuestos a consumir información transversal continúan haciéndolo en sus interacciones en línea[34]. Por otro lado, investigaciones recientes indican que las personas partidistas aumentan su polarización cuando se exponen a puntos de vista opuestos en las redes sociales[35].

Algunas personas obviamente se radicalizan a través de Internet; por ello, las plataformas de recursos más importantes se han centrado en combatir el reclutamiento terrorista en línea. Sin embargo, al abordar el problema del extremismo político, la pregunta es si los algoritmos de las plataformas son los verdaderos responsables de la radicalización. Existen pocos estudios rigurosos sobre el algoritmo de recomendación, e investigadores responsables llegan a conclusiones dispares: un estudio concluye que YouTube presenta un ligero sesgo algorítmico hacia la promoción de videos cada vez más radicales[36], mientras que otro sugiere que el volumen de contenido extremista simplemente ha aumentado en respuesta a la demanda y no como resultado de un sesgo algorítmico que ofrece a su audiencia materiales más radicales[37].

CONSECUENCIAS PARA LA ACCIÓN

Con miras a elaborar políticas eficaces que limiten cualquier posible daño, quienes se encargan de la formulación de políticas necesitan una base empírica sólida que fundamente la toma de decisiones. El mayor obstáculo para la comprensión de la repercusión que las redes sociales tienen en la diversidad de opiniones, o la radicalización de los puntos de vista, es la escasez de datos proporcionados por las plataformas a personas investigadoras expertas en la materia. Muchas de las investigaciones realizadas hasta la fecha se centran especialmente en los Estados Unidos y Europa, lo cual contrasta de forma radical con los limitados datos compartidos por las plataformas relativos a África, Asia y América Latina. Asimismo, disponemos de pocos datos en lo tocante a ciertas plataformas mucho más utilizadas en el Sur Global, como WhatsApp. Además, con relación a algunas cuestiones básicas como la radicalización a través de YouTube, la falta de accesibilidad de las investigaciones externas al algoritmo de recomendación nos impide evaluar si los cambios realizados por las plataformas durante el último año han tenido algún efecto en los resultados.

A fin de estudiar cualquiera de las patologías atribuidas a la transformación del ecosistema de medios digitales, estudios sociológicos necesitan acceder a datos controlados por las plataformas relacionados con “quién” visualizó o se interesó por “qué” y “cuándo”. Es decir, los científicos han de comprender el modo y el momento en que ciertas personas, y la población en general en distintos países, interactúan con los nuevos medios y cuáles son las consecuencias de esas interacciones. Aun cuando las plataformas se han comprometido a publicar datos para posibilitar la realización de investigaciones académicas independientes, a menudo no han cumplido dicha promesa[38].

Las autoridades públicas deben obligar a las principales plataformas de Internet a facilitar datos significativos sobre el impacto que los medios sociales tienen en la democracia a partes independientes. En especial, las plataformas deben compartir datos seguros y protegidos con instituciones académicas certificadas a fin de estudiar cuestiones como el análisis de algoritmos en materia de tendencias extremistas; la comprensión del efecto de los medios sociales en la polarización política y el consumo de información; y el esclarecimiento de la relación entre el discurso de odio en línea y la violencia física.

En vista del gran número de elecciones celebradas anualmente en todo el mundo y la variabilidad de la susceptibilidad de los países a la polarización tóxica, la desinformación y el discurso de odio, sería conveniente que la comunidad internacional que trabaja en el ámbito de la integridad electoral trabajase conjuntamente con las plataformas con miras a priorizar los países que requieren mayor atención y recursos con el fin de proteger su integridad electoral.

Dicha comunidad debe invertir en la creación de un índice de vulnerabilidad electoral que mida qué elecciones requieren un seguimiento estricto de las posibles injerencias electorales, el comportamiento falaz coordinado en línea y la desinformación.

III. EL DISCURSO DE ODIO Y LA INTEGRIDAD ELECTORAL

Internet facilita la coordinación y la acción colectiva entre grupos, incluso entre grupos extremistas en lugares geográficamente dispersos. Gab, 4chan, 8chan y subreddits, abiertamente racistas, se han convertido en medios populares para el debate, la construcción de una identidad compartida y la movilización entre grupos parias. El anonimato de estas redes facilita los debates ofensivos y el discurso de odio al tiempo que evita la rendición de cuentas. El auge de este discurso, que no entraña rendición de cuentas, ha generado preocupación por la relación entre las redes sociales y las nuevas olas de extremismo político, así como entre dichos medios y la violencia política.

En los últimos años, el vínculo entre el discurso de odio en línea y los abusos físicos se ha vuelto más evidente. En varias democracias occidentales, los defensores de la supremacía de la raza blanca utilizaron las redes sociales para publicitar tiroteos masivos dirigidos a minorías religiosas o raciales[39]. En la India, los rumores difundidos en WhatsApp provocaron linchamientos y violencia comunitaria; como resultado, decenas de personas fueron asesinadas[40]. En Sri Lanka, las publicaciones antimusulmanas difundidas en marzo de 2018 dieron lugar a actos violentos contra la minoría musulmana, lo que desembocó en la quema de cientos de casas y negocios[41]. En Myanmar, los agentes gubernamentales inundaron Facebook con discursos antimusulmanes y se mostraron a favor de la limpieza étnica de la minoría rohingya, lo que contribuyó al desplazamiento de 700.000 refugiados debido a las crecientes amenazas, los ataques físicos y la violencia sexual[42]. El riesgo de que las redes sociales extiendan el discurso de odio es especialmente peligroso para los países en el Sur Global, donde la combinación de las antiguas tensiones étnicas o religiosas y la rápida adopción de las nuevas tecnologías de la información puede intensificar los conflictos políticos.

El blanco del odio en la red son, especialmente, las mujeres. Según una encuesta reciente encargada por Amnistía Internacional, casi una cuarta parte (23%) de las mujeres en ocho democracias afirmaron haber sido víctimas del abuso o el acoso en línea, al menos una vez[43]. Del mismo modo, el Parlamento Europeo determinó que una quinta parte de las mujeres en la Unión Europea había sufrido acoso sexual en línea[44]. La intimidación por razón de género en línea puede ser una poderosa herramienta de autocensura que coarta la libertad de expresión y obstaculiza la participación democrática de los grupos contra los que se ejerce[45]. Amnistía Internacional afirma que la mayoría de las mujeres que han sido víctimas del abuso en línea han cambiado la forma en que utilizan las redes sociales; han ajustado su configuración de privacidad y modificado el contenido que publicaban[46] **[Recuadro 1]**. El efecto desmovilizador del abuso puede ser particularmente incisivo entre las periodistas y las candidatas políticas.

RECUADRO 1

Las redes sociales como instrumento contra las mujeres

Las redes sociales cada vez se instrumentalizan más y se emplean contra las mujeres periodistas, activistas y políticas mediante amenazas de violación y de violencias. Asimismo, la desinformación se utiliza para menoscabar la credibilidad y la capacidad de las voces femeninas prominentes que gozan de una posición importante en el ámbito de la política democrática. Por ejemplo, cuando Maria Ressa —una destacada periodista filipina— comenzó a cubrir el uso de propaganda del presidente Rodrigo Duterte en la campaña electoral filipina de 2016, su "ejército de teclado" empleó amenazas en línea, acoso selectivo y denuncias de corrupción, a fin de intimidarla[47]. Después de que Rappler, un popular medio de noticias, publicara la transcripción de una conversación telefónica entre el Presidente Trump y el Presidente Duterte, una red coordinada de bots y cuentas falsas inundó las redes sociales con el *hashtag* #ArrestMariaRessa (arrestar a Maria Ressa), lo que hizo que esta recibiera un flujo constante de mensajes de odio y amenazas. Incluso se le deseó que fuese "violada repetidamente hasta la muerte"[48].

La experiencia de Ressa con el troleo estatal, refleja la existencia de varias campañas emprendidas contra destacadas figuras femeninas de todo el mundo. Cuando la diputada ucraniana Svitlana Zalishchuk habló en las Naciones Unidas sobre el efecto de la Guerra en el Donbáss en las mujeres de Ucrania, una campaña de desinformación respaldada por la Federación de Rusia comenzó a difundir un tuit falso, supuestamente escrito por ella que decía que "correría desnuda por las calles de Kiev si el ejército ucraniano perdía una batalla clave"[49]. En las redes sociales, se difundieron imágenes manipuladas en las que aparecía desnuda, con miras a desacreditarla y avergonzarla aún más.

Estos ataques selectivos buscan silenciar la voz y reprimir la participación política de las mujeres a través de la vergüenza y la intimidación. A diferencia de otras formas de troleo, los ataques contra las mujeres suelen perdurar más tiempo y se centran en insultos degradantes y sexualizados, lo que los hace más viciados y duraderos. Las tácticas de intimidación cibernética por razón de género pueden convertirse en una herramienta poderosa para disminuir la libertad de expresión, e interrumpir la participación política de las mujeres dentro y fuera de la red[50].

El discurso de odio es una amenaza para la integridad electoral, ya que socava la seguridad mutua necesaria para garantizar el debate pacífico. También es una herramienta a disposición de candidaturas y partidos que avivan la violencia con el fin de suprimir el voto de sus oponentes. Esto supone una preocupación mayor en las democracias de transición en el Sur Global, que ya cuentan con un historial de violencia electoral y un estado de derecho débil que no garantiza la rendición de cuentas de los infractores.

ENFOQUES PARA REGULAR EL DISCURSO DE ODIO

Un obstáculo fundamental para la moderación del discurso de odio en línea consiste en la casi imposibilidad de definirlo y diferenciarlo de otros ejemplos de lenguaje ofensivo. Incluso cuando las plataformas crean una definición práctica, la complejidad y la variación dentro de las construcciones del lenguaje natural hacen que la detección automática del discurso de odio resulte imprecisa e incoherente. Si bien los líderes industriales y los encargados de formular políticas suelen coincidir en la necesidad de dedicar más esfuerzos a la lucha contra el discurso de odio, existen importantes discrepancias en cuanto a las medidas que se deben adoptar, dadas las dificultades relativas a la conceptualización y la aplicación. Es especialmente difícil separar el discurso de odio del discurso político legítimo, cuando los propios dirigentes de los países son partícipes precisamente de este tipo de juegos de palabras y, a veces, de discursos abiertamente racistas, lo que representa la base del tipo de censura que los críticos exigen a las plataformas.

El debate sobre el equilibrio entre la libertad de expresión y la protección de las personas contra la discriminación, es una cuestión de larga data. Sin embargo,

moderar el discurso de odio en la era digital es complicado debido al alcance extrajurisdiccional de las plataformas. Han surgido múltiples modelos regionales en respuesta a este problema, cada uno con una solución intermedia entre la protección de la libertad de expresión y la regulación del discurso, que podría justificar o incitar al odio y la violencia grupales.

El modelo de autorregulación es el más común en los Estados Unidos, donde el discurso de odio cuenta con protección jurídica gracias a la Primera Enmienda[51], y las plataformas de redes sociales están exentas de responsabilidad jurídica frente a casi todos los delitos, excepto los relacionados con la propiedad intelectual y los delitos federales[52]. Sin embargo, las compañías tecnológicas han tomado una serie de medidas encaminadas a limitar la difusión de contenidos que inciten al odio, entre los cuales están el cierre de cuentas, la eliminación y la degradación de cierto contenido, y la reducción del alcance de las ideas extremistas, contrarrestando la información con fuentes alternativas, mediante el uso de la inteligencia artificial y la moderación humana. El enfoque basado en la autorregulación tiene algunas limitaciones: los moderadores de Silicon Valley no necesariamente tienen el suficiente conocimiento cultural, político o religioso requerido para revisar el contenido que se comparte en el otro extremo del mundo[53], y la transparencia o la rendición de cuentas sobre el modo en que se aplican las decisiones técnicas y políticas es escasa[54].

En la Unión Europea se ha desarrollado un modelo más cuasi-normativo. Con arreglo a la legislación de la Unión Europea preexistente, las plataformas ya tenían la obligación de eliminar cualquier contenido ilegal, incluido el discurso de odio, previa notificación. En 2016, la Comisión Europea creó el *Código de Conducta para la Lucha contra la Incitación Ilegal al Odio en Internet*, en virtud del cual Facebook, Microsoft, Twitter y YouTube acordaron incorporar las prohibiciones del discurso de odio en sus directrices comunitarias. Así, el Código de Conducta se basa en las directrices comunitarias de las plataformas tecnológicas, como mecanismos formales de aplicación para suprimir el discurso de odio, según

lo define la legislación europea, estableciendo plazos específicos de respuesta a las notificaciones. En 2018, Instagram, Google+ y Snapchat también firmaron este Código de Conducta de la Unión Europea[55]. Esta iniciativa es relativamente poco intervencionista, en cuanto a que no creó un elemento regulador real cuya función sea la eliminación de contenido. Las organizaciones europeas de libertades civiles han criticado este marco por representar un sistema poco seguro, puesto que deja demasiado a discreción de empresas privadas[56]. Si bien el Código de Conducta de la Comisión esperaba crear redes de información y confianza entre la industria tecnológica, la sociedad civil y el gobierno, ha recibido valoraciones muy diversas.

Alemania ha dado un giro hacia una regulación gubernamental más directa, a través de la ley NetzDG de 2017. Esta protege a los usuarios alemanes de los medios sociales contra el discurso de odio y el acoso al hacer que las empresas de redes sociales se responsabilicen de atender las quejas de los usuarios en un plazo razonable[57], e imponiendo a las plataformas multas de hasta 50 millones de euros, por no eliminar contenido "claramente" ilegal dentro de las 24 horas posteriores a su notificación[58]. Sin embargo, la inmediatez del plazo de eliminación impide que éstas tengan en cuenta el contexto político y cultural de los contenidos que podrían considerarse como tales, de modo que coarta la libertad de expresión. En 2017, el Relator Especial de las Naciones Unidas sobre la libertad de opinión criticó la ley por incitar a la "censura cautelar" que "interfiere con el derecho a buscar, recibir e impartir información de todo tipo en Internet"[59]. Además, si los gobiernos autoritarios aplican leyes similares a NetzDG en su mandato, podrían justificar un aumento del control sobre la información[60] y menoscabar las normas internacionales de derechos humanos[61]. De hecho, ya se han aprobado leyes similares en la Federación Rusa y en la República Bolivariana de Venezuela, entre otros Estados autoritarios[62]. En casos más extremos, los gobiernos autoritarios aplican medidas como el cierre de Internet con el fin de controlar la información **[Recuadro 2]**.

RECUADRO 2

Las interrupciones del servicio de Internet en Asia y África

Los gobiernos autoritarios siguen aplicando interrupciones del servicio de Internet con el fin de sofocar las protestas políticas en Asia y África. En 2015, expertos internacionales en el plano jurídico de las Naciones Unidas, la Organización para la Seguridad y la Cooperación en Europa, la Organización de los Estados Americanos y la Comisión Africana de Derechos Humanos y de los Pueblos, condenaron estas acciones por coartar significativamente la libertad de expresión, restringir el acceso a la información y los servicios de emergencia en tiempos de disturbios. A pesar de ello, algunos políticos perpetúan una cultura de Internet que restringe la libertad, al obstaculizar el acceso a las redes sociales y a los foros en línea, como respuesta a las crisis[63].

Aproximadamente la mitad del total de interrupciones del servicio a escala mundial —incluidas las interrupciones intencionadas de las redes sociales, los servicios de telefonía móvil o el acceso a Internet— han tenido lugar en la India. Si bien el gobierno indio ha llevado a cabo estas acciones bajo el pretexto de sofocar la violencia durante los períodos políticamente polémicos en las últimas décadas, dichas medidas se han asociado con interrupciones de la acción colectiva tanto violenta como pacífica, por parte de los usuarios de Internet[64].

A raíz de los bombardeos de Pascua de 2019 en Sri Lanka, el Gobierno bloqueó el acceso a las páginas web de redes sociales, alegando objetivos similares. Aunque algunos medios de comunicación elogiaron al Gobierno por evitar la propagación del discurso de odio, análisis posteriores criticaron tan tajante decisión. En un país con medios relativamente débiles y no libres, la pérdida de la comunicación por Internet se sumó al caos y la confusión reinante. Además, los agentes maliciosos que intentaban difundir noticias falsas y un discurso violento, podían seguir propagando el odio por la región mediante redes virtuales privadas[65].

Las interrupciones del servicio de Internet en África han aumentado en los últimos años. Más de una decena de países africanos han interrumpido el acceso a internet durante las elecciones o a lo largo de períodos de disidencia política, como Egipto[66], el Togo y Etiopía. Un estudio realizado sobre diez países de África Subsahariana reveló que los apagones no solo fueron peligrosos, sino también costosos; las interrupciones efectuadas entre 2015 y 2017 provocaron una pérdida estimada de 235 millones de dólares en dichos países[67].

Sorprendentemente en Uganda y Benin, las interrupciones se sumaron a la inequívoca represión estatal. Justo antes de las elecciones de 2016 en Uganda, la Comisión Electoral del Estado interrumpió el acceso a Facebook, Twitter y foros similares; durante este tiempo, el Estado mantuvo a dos candidatos presidenciales bajo arresto domiciliario y no restableció el acceso completo a Internet hasta que la votación había concluido. Los críticos argumentaron que esto permitió que el Gobierno se protegiera de las críticas por injerencia en los procedimientos electorales[68]. En Benin, un país famoso por su carácter estable y democrático, las autoridades electorales dictaminaron de manera similar que los candidatos de cinco partidos de la oposición, contrarios al Presidente Talon, no podían presentarse a las elecciones parlamentarias de 2019. El Gobierno tomó medidas estrictas contra la indignación y las protestas públicas, cerró ciertas páginas web de redes sociales y, en última instancia, bloqueó todo el acceso a Internet el día de las elecciones[69].

Estos ejemplos son algunos de los que han amenazado el acceso a la información y las libertades electorales en Asia y África. Si bien las redes sociales y otros foros de comunicación en línea plantean retos para los reguladores, las cada vez más frecuentes interrupciones llevadas a cabo por regímenes autoritarios, refuerzan el valor de estas tecnologías para los activistas en favor de la democracia.

En particular, ninguno de estos modelos ofrece un marco normativo claro que permita afrontar la "generalización" del discurso de odio en muchos países y su cada vez mayor integración en el diálogo político habitual, así como en el discurso de numerosas élites políticas prominentes. Los gobiernos aún no han encontrado una forma para que las plataformas aborden esta tendencia, sin interferir en las campañas electorales o tomar decisiones partidistas, sobre qué discurso político ha de censurarse.

CONSECUENCIAS PARA LA ACCIÓN

En los diferentes regímenes normativos existen distintos principios sobre cómo, cuándo y por qué se debe eliminar el discurso de odio de las redes sociales. Sin embargo, en todos ellos, las plataformas tecnológicas deben intensificar sus esfuerzos para adaptar sus prácticas al tamaño de su mercado. Aún existen diversas limitaciones que impiden la implementación de soluciones basadas en inteligencia artificial, especialmente cuando se aplican al Sur Global y las regiones en las que el inglés no es el idioma principal. Al mismo tiempo, las plataformas tienen la responsabilidad de garantizar el cumplimiento de los mismos estándares de moderación del contenido a escala mundial, y deben prestar especial atención a las comunidades vulnerables a los conflictos étnicos, los disturbios y los delitos de odio. En estos contextos, las plataformas deben invertir especialmente en el desarrollo de sistemas de alerta temprana, que permitirían identificar el contenido que puede representar una amenaza potencial para las elecciones, y someterlo a revisión por parte de personas físicas, antes de que alcance cierto nivel de viralidad. Las empresas tecnológicas deben asignar más recursos a la moderación automática de contenidos, la traducción de textos, la competencia cultural en materia de moderación humana y otras herramientas similares, con miras a garantizar que sus usuarios gozan de igualdad de oportunidades para participar en el discurso político en línea. Asimismo, deben proporcionar más datos sobre la medida en que el

discurso de odio constituye un problema en sus plataformas. Si bien los informes de transparencia proporcionan estadísticas generales sobre el número de contenidos eliminados, comprender mejor el tipo de publicaciones que se identifica y elimina no solo ayudará a mejorar los sistemas de alerta temprana, sino que también contribuirá a fundamentar la formulación empírica de políticas, a fin de proteger a las comunidades más vulnerables contra el discurso de odio, el acoso y los abusos.

Las plataformas de redes sociales deben desarrollar sistemas de alerta temprana con miras a detectar la desinformación electoral, la injerencia extranjera, los delitos de odio, las amenazas contra las mujeres, la violencia y la supresión de los votantes.

Las plataformas han de contar con más expertos con dominio de los idiomas locales y competencia cultural del lugar donde trabajan.

Puesto que cuando la comunicación ya se ha hecho viral es demasiado tarde para tomar medidas, los sistemas de alerta temprana deben comenzar a aplicar la revisión por parte de personas físicas de las cuentas y las publicaciones que representan una posible amenaza para las elecciones. Una persona física ha de encargarse de la revisión y del control del contenido que, en mayor o menor medida, se hace viral.

Los gobiernos deben obligar a las plataformas de redes sociales a actualizar los informes de transparencia, con miras a hacer públicos los datos relativos al número de denuncias de discurso de odio y abusos en línea. Se deben incluir datos sobre los casos de abuso selectivo (por razón de género, raza, orientación sexual o religión), y la frecuencia con que distintas comunidades se ven afectadas.

Un obstáculo importante para la intensificación de los esfuerzos en favor de la moderación es la diversidad de los expertos que diseñan las tecnologías de revisión de contenido. Los algoritmos, la inteligencia artificial y otras tecnologías no son herramientas neutrales; incorporan los valores y los prejuicios de sus creadores y usuarios. Un creciente número de trabajos empíricos han mostrado cómo estos

prejuicios inherentes a las tecnologías y las prácticas empresariales pueden dar lugar a decisiones automatizadas incoherentes, y a menudo discriminatorias[70]. Y aun así, la mayoría de los ingenieros que idean la próxima generación de tecnologías son jóvenes blancos de Silicon Valley. Parte de la solución a largo plazo implicará garantizar que los ingenieros y los líderes industriales cuentan con experiencias y orígenes diversos, para lo cual se requerirá una inversión a largo plazo en la diversificación de los ámbitos de la informática, la ingeniería y la ciencia de datos **[Recuadro 3]**. Esta inversión fortalecerá la integridad electoral —en términos generales— y otorgará poder de decisión sobre el diseño de la plataforma a un grupo de expertos, que represente más fielmente las características demográficas y culturales de los usuarios de los medios sociales.

Las autoridades públicas, las organizaciones internacionales, las fundaciones filantrópicas y la sociedad civil deben ayudar a las democracias a desarrollar programas de tecnología cívica a través de la formación en codificación, especialmente para las mujeres y las minorías, y mediante la incorporación de personal con habilidades técnicas en los equipos gubernamentales.

Los ciudadanos, la sociedad civil y el gobierno también pueden intensificar sus esfuerzos en favor de la promoción de un entorno saludable en la red, de manera que contribuyan a aumentar el porcentaje de diálogo político respetuoso y de calidad. Las actuaciones de las organizaciones de la sociedad civil en Kenya durante las elecciones de 2013, encaminadas a reducir el discurso de odio en línea, fueron impresionantes. Al crear un entorno de empoderamiento que permitió a la ciudadanía contrarrestar, desacreditar y avergonzar a quienes compartían discursos violentos, las organizaciones de la sociedad civil finalmente pudieron reducir la proporción de este tipo de actitudes y crear un entorno electoral centrado en el diálogo no violento **[Recuadro 4]**.

La comunidad que trabaja en el ámbito de la integridad electoral debe proporcionar financiación a organizaciones de la sociedad civil que luchan contra el discurso de odio, el acoso selectivo y la incitación a la violencia, especialmente en el período previo a las elecciones.

RECUADRO 3

Iniciativas en favor de la diversidad en la codificación

La integridad electoral requiere un acceso equitativo a la participación política entre los grupos sociales marginados. Sin embargo, debido a los abusos en línea, las poblaciones vulnerables se sientan inseguras, su participación en el debate político en línea disminuye y, en casos extremos, sus carreras políticas o periodísticas resultan insostenibles. El diseño algorítmico y las herramientas de moderación de contenido actuales apenas responden a las preocupaciones relativas al discurso de odio y el acoso. Una solución a largo plazo consiste en aumentar significativamente la diversidad entre los ingenieras/os y líderes en tecnología que desarrollan los algoritmos y toman decisiones en materia de contenido.

En los últimos años, algunas organizaciones sin ánimo de lucro se han centrado en el desarrollo de proyectos de capacitación tecnológica; estas iniciativas ayudarán a extender la toma de decisiones a las comunidades marginadas más afectadas por los sesgos algorítmicos y los ineficaces sistemas de moderación del contenido. Se incluyen, entre otras, organizaciones destacadas cuyo objetivo es aumentar la presencia de las mujeres en el ámbito tecnológico —como Girls Who Code, Grace Hopper Program y Women Techmakers—, así como programas dirigidos a las minorías —incluidos Black Girls Code; #YesWeCode; y Algorithmic Justice League—.

Un modelo de éxito es Girls Who Code, una organización sin ánimo de lucro cuyo objetivo es aumentar el número de mujeres presentes en la esfera de la informática y la ingeniería, ofreciendo una variedad de programas de codificación dirigidos a las niñas. Esta organización dirige programas extracurriculares durante el año académico con el fin de impartir formación informática en ámbitos como la programación, la robótica, el diseño web y el desarrollo de aplicaciones[71]. Según su informe anual de 2018, el porcentaje de antiguas alumnas del programa que se especializan en ámbitos relacionados con la informática supera casi quince veces el porcentaje nacional[72]. Estas iniciativas formativas están ganándose el apoyo de las principales empresas tecnológicas; entre las empresas patrocinadoras de Girls Who Code se encuentran Google, Twitter y GE[73].

RECUADRO 4

El seguimiento ciudadano del discurso de odio en Kenya, 2012-2013

Las elecciones presidenciales de Kenya de 2007 desencadenaron dos meses de violencia generalizada. Más de 1.200 personas fueron asesinadas y más de 600.000 se vieron obligadas a abandonar sus hogares[74].Las pruebas anecdóticas sugieren que el prolífico discurso de odio en línea contribuyó a la adopción de un comportamiento violento[75].

En los meses previos a las elecciones de 2013, más de 477 personas fueron asesinadas en actos violentos entre comunidades, en medio de una retórica incendiaria en torno a las controversias sobre la propiedad de la tierra. La Comisión Nacional de Cohesión e Integración del Gobierno, posterior a 2007, encargada de juzgar a los defensores del discurso de odio, tuvo dificultades para definir o aplicar sus propias políticas[76]. Sin embargo, la violencia se desvaneció durante las elecciones gracias a la acción colectiva de la sociedad civil, que adoptó enfoques innovadores para combatir el discurso de odio.

Denominadas coloquialmente “propaganda por la paz”, las organizaciones de la sociedad civil difundieron llamados en favor de la paz y la unidad a través de las redes sociales, de carteles y campañas publicitarias. Una iniciativa de mensajes de texto sin ánimo de lucro envió mensajes estratégicos a 65.000 ciudadanos kenianos en favor de la paz. El popular programa de televisión *Vioja Mahakamani* emitió cuatro episodios especiales centrados en el diálogo no violento. Las investigaciones posteriores descubrieron que estos episodios aumentaron significativamente el escepticismo de los espectadores con respecto al discurso de odio[77].

Algunos grupos elaboraron programas pilotos de seguimiento del discurso de odio que permitieron a los individuos actuar contra éste en los foros en línea. Se puso en práctica una iniciativa,

llamada *Proyecto Umati*, de septiembre de 2012 a mayo de 2013. Tras visitar los sitios web más populares en Kenya, un equipo de seguimiento identificó casi 6.000 casos de discurso de odio. Dicho equipo constató que una cuarta parte de estos casos hacían llamados "muy peligrosos" a la violencia y que más del 80% de los casos de incitación al odio se registraban en Facebook[78].

Esta investigación dio lugar al proyecto *Nipe Ukweli*, que difundió instrucciones para el seguimiento ciudadano del discurso de odio a través de las redes sociales, los medios tradicionales y los foros comunitarios. Los folletos describían las características del discurso de odio y alentaban a la ciudadanía a denunciar a los usuarios que ejercían los abusos a través de un chat de asistencia y una base de datos en Internet. Disponible en inglés y swahili, el proyecto hacía hincapié en la capacidad de elección y el poder de la ciudadanía para contrarrestar, desacreditar o simplemente desvincularse del discurso violento[79].

IV. LA PROTECCIÓN DE LA INTEGRIDAD ELECTORAL CONTRA LA DESINFORMACIÓN

La desinformación, definida como la difusión intencionada de información falsa o engañosa, se ha convertido en una amenaza crítica para la integridad electoral. En los últimos años, una gran variedad de agentes con motivaciones de carácter político y económico ha empleado las redes sociales con el fin de difundir y aumentar la desinformación y la propaganda entre los posibles votantes antes de las elecciones en todo el mundo, exacerbando las antiguas divisiones étnicas, religiosas y sociales, y sembrando la desconfianza en los medios de comunicación y las instituciones democráticas.

Desde un punto de vista normativo, queremos que el electorado tome decisiones fundamentadas. Cuando las y los votantes están mal informados, corren el riesgo de elegir candidaturas que realmente no se adhieren a sus preferencias. Deben comprender las consecuencias de sus decisiones y poder exigir responsabilidades a sus representantes. La desinformación puede, por lo tanto, eliminar la rendición de cuentas de las elecciones. Sin embargo, más allá de las cuestiones normativas, la desinformación puede disminuir directamente la integridad electoral al menoscabar la seguridad mutua. Asimismo, puede socavar la confianza en unas elecciones libres y limpias, al sembrar dudas sobre la integridad de las urnas y el comportamiento profesional e imparcial de los órganos electorales, y al difundir rumores que cuestionan la legitimidad y la fiabilidad de las elecciones.

La desinformación no es un fenómeno nuevo ni es exclusivo de las tecnologías de la información y las comunicaciones actuales[80]. Los argumentos que enmarcan la desinformación como un problema únicamente relacionado con las “redes sociales” desvían la atención de la responsabilidad de los medios tradicionales y los políticos a la hora de crear un ecosistema informativo en el que prosperan la desinformación y el discurso de odio. En los países en los que los medios tradicionales son extremadamente partidistas, la ciudadanía observa cómo la prensa, la televisión o la radio amplían el alcance y legitiman algunos de los peores rumores y casos de desinformación que se pueden encontrar en línea.

Incluso aquellos países en los que los medios tradicionales son en gran medida responsables y objetivos pueden ser proclives a la desinformación en línea o a la difusión de un discurso que debilite la confianza y la integridad electoral.

Sin embargo, las redes sociales suelen constituir el lugar en el que los usuarios encuentran historias falsas o engañosas[81], lo cual se debe, en parte, a que estos medios han cambiado radicalmente la forma en que se producen y consumen las noticias y la información. Es obvio que, en la era digital, cualquiera que cuente con un teclado puede publicar información.

Los microblogs y el periodismo ciudadano han proporcionado mayores oportunidades de llegar a un público más amplio, en tiempo real, a través de noticias y contenidos. Además, los medios tradicionales y las organizaciones de radiodifusión —que proporcionan barreras de seguridad en el ámbito de la comunicación política— ya no tienen el monopolio de la difusión informativa[82]. Si bien las redes sociales empoderan a los usuarios como productores de información, el declive de los intermediarios "de control" tradicionales ha provocado que las normas que rigen los medios heredados no siempre se apliquen al arsenal de contenido generado por los diferentes usuarios. Por lo tanto, la desinformación —y otras formas de contenido de baja calidad, extremadamente partidista o conspirativa— puede apropiarse fácilmente de las redes sociales.

Los algoritmos de las redes sociales, y las políticas y prácticas que rigen su uso, también contribuyen a la forma en que

la desinformación se difunde en línea. El entorno actual de la información digital se "conforma mutuamente" mediante algoritmos que ordenan, clasifican, priorizan y envían contenido, y usuarios que influyen en el tipo de recomendaciones que los algoritmos producen a través de los datos generados por sus interacciones en línea[83]. Los algoritmos no son tecnologías neutrales[84]; más bien, son infraestructuras publicitarias y persuasivas, diseñadas con el objetivo de maximizar la atención del usuario y, posteriormente, los ingresos publicitarios[85]. Puesto que las personas se sienten atraídas por contenidos emotivos, vívidos y convincentes, tanto los algoritmos que maximizan la atención como las preferencias humanas tienden a favorecer los hechos ficticios y tentadores ante la tediosa realidad. Además, la desinformación —que está diseñada expresamente para despertar reacciones contundentes y emocionales— puede generar un compromiso mucho mayor que otras formas de noticias e información[86].

Recientemente, dos acontecimientos de gran repercusión han ejemplificado la preocupante relación entre las redes sociales y la desinformación: el referéndum del Brexit de junio de 2016 en el Reino Unido, y las elecciones presidenciales de noviembre de 2016 en los Estados Unidos. Las llamadas noticias falsas que sirven para generar titulares escandalosos, como la supuesta participación de Hilary Clinton en una red de pedófilos en el sótano de una pizzería de Washington D. C., ocuparon un lugar destacado en las redes sociales de algunos usuarios. Muchas de estas "noticias falsas" tuvieron mayor repercusión que las noticias profesionales[87], lo que distrajo a la ciudadanía de otros importantes debates públicos sobre las elecciones. Si bien este tipo de falacias como el "#Pizzagate" o "el apoyo del Papa a la presidencia de Donald Trump" contenían información claramente susceptible de ser falsificada, la desinformación suele combinar hechos verídicos y ficticios, de tal manera que se dificulta el discernimiento entre qué es real y qué no. No toda la desinformación es completamente falsa: puede emplearse información objetiva para "desacreditar puntos de vista opuestos" o tergiversar los hechos[88]. A este problema se suma el uso de la sátira, la parodia y la exageración, que algunos pueden interpretar como

elementos humorísticos, mientras que otros pueden considerarlos noticias[89]. ¿Se deben incluir los errores informativos, la sátira política y las declaraciones erróneas de los políticos dentro de la definición de desinformación, o sólo ha de tenerse en cuenta la información claramente falsificada? Se ha demostrado que los intentos por llegar a una posición intermedia y calificar las posibles noticias falsas como "controvertidas" tiene consecuencias no deseadas, como hacer que las historias no calificadas como tales, parezcan más fiables y contrastadas[90].

LA MEDICIÓN DE LA PREVALENCIA DE LA DESINFORMACIÓN

La forma en que se define el problema de la desinformación repercute significativamente en la estimación de su prevalencia. No obstante, contrariamente a lo que a veces se afirma, las democracias no están ahogándose en un mar de desinformación. La investigación empírica sobre la prevalencia real de la desinformación sigue siendo escasa, y los estudios existentes tienden a aplicar definiciones dispares de la desinformación, o centrarse especialmente en los Estados Unidos, lo que hace difícil establecer generalizaciones sobre la desinformación. Sin embargo, cada vez existen más pruebas que nos recuerdan que la escala de la desinformación es distinta en todo el mundo, en las plataformas y entre las comunidades de usuarios. Sobre la base de una definición estricta de "noticias falsas", Allcott y Gentzkow estimaron que en el período previo a las elecciones presidenciales de los Estados Unidos de 2016 en promedio cada adulto estadounidense leyó y recordó al menos un artículo de noticias falsas en las redes sociales[91]. Otro estudio de Guess, Nyhan y Reifler estimó que aproximadamente el 27% —es decir, 65 millones— de los estadounidenses estuvieron expuestos

a, como mínimo, un artículo de noticias falsas durante un período de tiempo similar[92]. De acuerdo con un enfoque de definición más amplio, Howard *et al.* determinaron que los usuarios de Twitter en los Estados Unidos compartieron tantas "noticias basura" —o contenido de carácter conspirativo, extremadamente partidista y carente de respeto por algún estándar periodístico profesional— como noticias profesionales en las dos semanas previas a las elecciones presidenciales de 2016[93].

Sin embargo, la prevalencia de las "noticias falsas" o "basura" en los medios sociales varía a lo largo del mundo. En el Reino Unido, Francia y Alemania, los usuarios de Twitter compartieron un porcentaje significativamente mayor de noticias profesionales (el 49%, el 46% y el 40%, respectivamente) que de noticias falsas (el 10%, el 4% y el 9%, respectivamente)[94]. En Suecia, uno de cada tres localizadores de recursos uniformes (URL) compartidos en Twitter se clasificaba como noticia basura[95]. En el Brasil, solo el 1,2% del total del contenido compartido en Twitter sobre las elecciones de 2018 fueron noticias basura[96]. Sin embargo, en dicho país, un estudio simultáneo de comunicación política en WhatsApp mostró un panorama diferente: en WhatsApp, aplicación utilizada por el 90% de los usuarios brasileños de Internet, la desinformación se manifestaba en forma de contenido visual a través de memes, imágenes y enlaces a videos de YouTube[97]. De las 50 imágenes más compartidas en grupos públicos de WhatsApp, solo cuatro contenían información verídica[98]. El análisis cualitativo mostró que la desinformación en WhatsApp aprovechó y exacerbó las divisiones políticas y avivó el sentimiento antifeminista y anti-LGBTQ[99]. Se identificaron patrones similares de comunicación política en la India, donde WhatsApp tiene más de 200 millones de usuarios; una tercera parte del total de imágenes compartidas por el Partido Bharatiya Janata y una cuarta parte de las imágenes compartidas por el Congreso Nacional Indio fueron clasificadas como divisionistas y conspirativas[100].

Más allá de las diferencias entre un extremo u otro del mundo y dentro de las plataformas, también existen disparidades entre el público que comparte y consume información falsa. Si bien para los usuarios más jóvenes a veces resulta difícil juzgar la credibilidad de la información en línea, la difusión y el consumo de la desinformación tiende a ser generacional y partidista. En los Estados Unidos, se concluyó que los usuarios que se identificaban como políticamente conservadores eran más propensos a compartir noticias falsas que los liberales o moderados[101]. No obstante, la edad también constituía un factor importante: las personas mayores de 65 años eran quienes compartían más "noticias falsas", independientemente de su ideología o afiliación política[102]. Esto se refleja en otros países, como Nigeria, donde los usuarios de mayor edad dieron una difusión más amplia a las noticias falsas en WhatsApp[103].

LA INSTRUMENTALIZACIÓN DE LA DESINFORMACIÓN

Si bien las investigaciones actuales no proporcionan datos claros sobre el grado de difusión de la desinformación en las redes sociales, los agentes maliciosos han instrumentalizado cada vez más la desinformación con fines políticos o económicos. Mediante las ventajas de la viralidad y el anonimato que ofrecen las plataformas de redes sociales, las redes coordinadas de cuentas falsas han utilizado la desinformación para contaminar la esfera pública digital y exponer a los usuarios moderados a noticias que parten de ideas marginales. Esto ocurre a menudo de manera orgánica, generando un compromiso inauténtico a través de redes automáticas y coordinadas de cuentas falsas que dan a "me gusta", comparten, retuitean y reenvían mensajes con la intención de convertirlos en virales. En muchas democracias, hemos observado cómo se emplea la "propaganda computacional" con el fin de aumentar la cantidad de desinformación, vídeos y memes políticos para infundir miedo, ira e indignación, lo que, en algunos casos, ha llegado

a provocar violencia y disturbios políticos. A medida que avanzan las innovaciones tecnológicas, incluida la inteligencia artificial y el análisis de macro-datos, las herramientas y técnicas de desinformación también evolucionan. Ya hemos visto ejemplos de imágenes, vídeos y audios toscamente manipulados y difundidos en la red, como el vídeo viral de la Presidenta de la Cámara de Representantes de los Estados Unidos, Nancy Pelosi, que fue editado para que pareciera que estaba ebria. También existen tecnologías que utilizan la inteligencia artificial para emular la expresión facial, el movimiento corporal y la modulación de la voz; estas podrían cambiar aún más el panorama de la información digital, especialmente porque las empresas de redes sociales ya tienen dificultades para evitar que el contenido nocivo se difunda en sus plataformas.

CONSECUENCIAS PARA LA ACCIÓN

La creciente preocupación sobre la prevalencia, el efecto y la instrumentalización de la desinformación, ha ejercido una fuerte presión sobre los encargados de la formulación de políticas, con el objetivo de que "tomen cartas" en el asunto. Desde 2016, más de 40 gobiernos han propuesto o aplicado nuevas leyes diseñadas para abordar el fenómeno de las "noticias falsas" en las redes sociales[104]. Sin embargo, esta presión —junto con la capacidad de proporcionar una respuesta rápida a un problema complejo de múltiples facetas— constituye un serio desafío, pues las investigaciones solo han podido analizar de manera superficial lo que sabemos de la desinformación. En este sentido, aún es escasa la investigación con base empírica que permita entender quién comparte la desinformación, por qué la comparte, y si es consciente de que se trata de información falsa[105]. Incluso menos estudios explican los efectos de la exposición a la desinformación y en qué medida tal exposición fomenta o no la polarización, el partidismo, el extremismo o la violencia. Asimismo, en un ecosistema mediático híbrido, es difícil determinar el efecto específico de las redes sociales en la democracia[106].

Al considerar el papel gubernamental y de las empresas de redes sociales en la regulación de la desinformación —y, en última instancia, la expresión— en línea, es preciso analizar también el contexto mundial en el que operan las plataformas. En algunos países —en los que las instituciones son débiles, existe restricción de los derechos humanos, y se infringen de manera habitual las normas democráticas—, las plataformas de redes sociales pueden convertirse en motores normativos eficaces que impulsen los valores democráticos. Las redes sociales tienen su valor como espacio para la expresión, la organización, la protesta y el intercambio de información —en especial para quienes viven en regímenes cerrados o represivos—. Sin embargo, el empoderamiento de las empresas como "árbitros de la verdad" también conlleva perjuicios considerables y, por consiguiente, los beneficios derivados de reducir la exposición a la desinformación deben ser sustanciales para justificar la concesión de semejante poder de control de la expresión a empresas cuyo propósito es obtener el máximo beneficio[107].

A fin de garantizar la integridad de los procesos electorales, es importante que la ciudadanía tenga acceso a información verificada de gran calidad. Si bien agentes malintencionados han intentado desbordar el ecosistema digital con desinformación, también se han observado ejemplos positivos de organizaciones de la sociedad civil que trabajan para combatir esta situación. Cabe destacar la impresionante labor de cooperación emprendida en períodos electorales por organizaciones de la sociedad civil, medios de comunicación tradicionales y plataformas tecnológicas con el fin de desmentir las noticias falsas y detener su propagación en países como México e Indonesia [véanse los Recuadros 5 y 6]. Tales iniciativas requieren gran cantidad de tiempo y esfuerzo, pero los hechos sugieren que las organizaciones nacionales dedicadas a defender la integridad electoral pueden resultar de gran eficacia a la hora de facilitar el acceso de la ciudadanía a ellas, fomentar la confianza en su criterio, y desacreditar con éxito los casos de desinformación flagrantes. Estas medidas resultan más eficaces cuando los medios de comunicación tradicionales valoran la objetividad y los órganos de gestión electoral advierten adecuadamente a la ciudadanía de la amenaza que representan las noticias falsas.

La comunidad que trabaja en el ámbito de la integridad electoral debe contribuir a desarrollar las capacidades de las organizaciones nacionales con el objetivo de defender la integridad de las elecciones frente a la instrumentalización de la desinformación, y apoyar la mejora de las prácticas de evaluación e intercambio de información.

Asimismo, es importante considerar la aplicación de respuestas políticas que limiten la capacidad de los agentes malintencionados para instrumentalizar las plataformas de redes sociales y generar un alcance falso. La naturaleza anónima y pseudoanónima de las redes sociales ha permitido que estos agentes creen redes de cuentas falsas capaces de multiplicar la velocidad y la escala de la difusión de desinformación. La Comisión considera el anonimato un elemento esencial de la democracia y la integridad electoral, ya que representa una valiosa barrera de seguridad en los países que carecen de las protecciones de los derechos humanos fundamentales para la participación democrática. No obstante, cuando se combina con la automatización, el anonimato puede plantear grandes riesgos para la esfera pública digital. En lugar de reducir el nivel de anonimato ofrecido por Internet y las plataformas de medios sociales, las empresas deben aumentar la transparencia en relación con las cuentas automatizadas. Una mayor atención a la transparencia en la identificación de las cuentas automatizadas contribuirá a la evaluación de la popularidad de las fuentes de información y a determinar si cierto contenido ha sido exagerado artificialmente, a la par que se preserva el anonimato esencial para la participación democrática.

Los gobiernos deben obligar a las plataformas a identificar las cuentas automatizadas. Cuando las plataformas no identifiquen correctamente las cuentas automatizadas (p. ej., un bot), deben enfrentarse a sanciones económicas impuestas por las autoridades públicas.

La instrumentalización de la desinformación afecta al conjunto del ecosistema mediático. Aunque una campaña puede empezar en una sola plataforma, las mismas imágenes, memes, vídeos o direcciones URL se pueden compartir en

otras. Las plataformas deben esforzarse más por coordinar sus respuestas ante las campañas de instrumentalización de la desinformación, lo cual requerirá mayor colaboración entre las empresas con el fin de identificar el contenido sospechoso y las redes de cuentas que lo comparten. La responsabilidad de luchar contra el comportamiento falaz coordinado no debe limitarse a las plataformas como entes individuales. A fin de fomentar la integridad electoral, es necesario mejorar el intercambio de información y las estrategias entre plataformas para detectar y limitar el alcance de la desinformación y la incitación al odio.

Las plataformas de redes sociales deben crear una coalición con el propósito de afrontar las amenazas digitales a la democracia y la integridad de los procesos electorales, de manera similar a la colaboración mantenida en el ámbito de la lucha contra el terrorismo y la explotación infantil. Los miembros de las coaliciones han de reunirse con regularidad y crear estrategias para múltiples plataformas orientadas a detectar y limitar el alcance de la instrumentalización de la desinformación.

A largo plazo, las sociedades democráticas deben trabajar para protegerse contra la instrumentalización de la desinformación. La ciudadanía de la era digital tendrá que convertirse en experta en información, propaganda y fuentes en línea[108]; deberá saber cómo reconocer las falacias e identificar las teorías conspirativas. La capacidad para averiguar quién está detrás de una página web específica y qué defiende es un elemento crucial de la educación digital; sin embargo, tan importante es formar a la ciudadanía para que sepa reconocer la posible procedencia de la información, como capacitarla para que identifique el origen potencial de su propia parcialidad. Hemos de aspirar a que los votantes se pregunten: "¿de dónde procede esta información y qué intereses fomenta?". No obstante, es igual de importante que se pregunten: "¿por qué tengo predisposición a creer o descartar esta información?".

Las autoridades públicas deben promover los programas de alfabetización digital y mediática en las escuelas y la programación de interés público entre la población en general.

RECUADRO 5

El enfoque de México para combatir la desinformación

El Instituto Nacional Electoral (INE) de México se encontraba bien preparado para luchar contra las noticias falsas que podían influir en la opinión de las y los votantes, erosionar la confianza pública en los procesos electorales, o incrementar la polarización y fragmentación durante las elecciones que tuvieron lugar en el país en 2018[109]. A lo largo del ciclo electoral, el INE siguió una estrategia tripartita eficaz dirigida a forjar una "alianza" con las empresas mediáticas—especialmente las de redes sociales—, apoyar la iniciativa *Verificado 2018* de la sociedad civil, y establecer un sistema informático de verificación de datos, CERTEZA 2018, para desmentir la información falsa en línea[110].

Mediante un único esfuerzo coordinado, el INE estableció acuerdos de cooperación formales con Facebook, Twitter y Google, lo que posibilitó la primera transmisión en directo de los debates presidenciales mexicanos y los anuncios electorales del INE, que siguieron millones de votantes en todo el país[111]. Además, el INE colaboró con Facebook para implementar "botones" interactivos que permitían a los usuarios acceder al sitio web de la autoridad electoral oficial y, de ese modo, difundir mensajes de promoción del voto, así como contar con la participación de los usuarios en la selección de los temas de debate[112]. De manera similar, Google incluyó un botón para redirigir a los usuarios hasta el contenido del sitio web del INE, y alojó una aplicación de Google Maps para ofrecer a los votantes información sobre la ubicación de las mesas de votación[113]. Twitter y el INE establecieron de forma conjunta discusiones sobre el debate presidencial y emplearon hashtags rastreables, crearon un foro para proporcionar comentarios periodísticos en tiempo real, y utilizaron una función de respuesta automática a fin de ofrecer los resultados de las elecciones en tiempo real[114].

Asimismo, el INE apoyó la iniciativa de verificación de datos *Verificado 2018*, que, dirigida por Animal Político, AJ+ Español, Newsweek Español y Pop-Up Newsroom, consiguió reunir a más de 60 organizaciones de la sociedad civil. *Verificado* creó un canal de WhatsApp, junto con toda una serie de foros de redes sociales adicionales, para que los usuarios consultaran la veracidad de las declaraciones políticas y recibieran respuestas fiables en un plazo de tiempo razonable. Los operadores del proyecto consiguieron responder a 400 consultas, crear 50 vídeos informativos, y atraer a millones de visitantes a su sitio web oficial[115].

Además, el INE estableció CERTEZA 2018, un mecanismo tecnológico; mediante el uso de sistemas informáticos y humanos de seguimiento, operadores sobre el terreno y un equipo de evaluación, CERTEZA hizo frente a la información falsa en cinco fases, a saber: 1) seguimiento de la información falsa mediante palabras clave; 2) evaluación de los casos identificados; 3) verificación de los cursos de acción apropiados; 4) recopilación de pruebas; y 5) difusión de avisos en los medios tras la evaluación de casos[116]. A la hora de difundir la información verificada, CERTEZA se benefició de los acuerdos de cooperación con las plataformas mediáticas, así como de la capacidad de alcance de *Verificado*. Tras realizar un seguimiento de millones de publicaciones en redes sociales, el sistema consiguió identificar 217 casos de instrumentalización política de la desinformación el día de las elecciones, al mismo tiempo que respondía a las solicitudes de los usuarios que precisaban información específica sobre las elecciones[117].

Además de iniciar y respaldar estas vías para combatir la desinformación, el INE se protegió contra los ciberataques mediante 2.000 auditorías del sistema informático y una vigilancia en tiempo real ininterrumpida[118]. En conjunto, el enfoque empleado por el INE durante las elecciones de 2018 representa un modelo innovador y eficaz que otras naciones pueden emular en procesos electorales futuros.

RECUADRO 6

El enfoque de Indonesia para combatir la desinformación, 2018-2019

En Indonesia se registró un aumento de la prevalencia de noticias falsas durante las elecciones de 2018-2019[119]. Los órganos electorales del país respondieron a la situación mediante una serie de iniciativas en colaboración con organizaciones de la sociedad civil, organismos públicos competentes y plataformas de redes sociales. Estas asociaciones, que se centraron en la lucha activa contra la desinformación y el discurso de odio, así como en salvaguardar la confianza pública en las elecciones, incluían actividades de sensibilización, aplicación de disposiciones jurídicas y normativas, e iniciativas conjuntas de verificación de datos.

Los dos órganos electorales —la Comisión Electoral General y la Agencia de Supervisión Electoral— junto con organizaciones de la sociedad civil, incluida la Comunidad Indonesia Antidifamación y el Centro para el Estudio de la Religión y la Democracia de la Fundación Paramadina, desarrollaron estrategias para combatir la desinformación en el contexto indonesio. Su labor se benefició de las mejores prácticas compartidas por la Fundación Internacional para Sistemas Electorales (IFES) basadas en su experiencia más reciente en este ámbito en Kenya[120]; entre otras, contar con la participación de diversas partes interesadas; sensibilizar; recopilar datos; desarrollar contrapropaganda; y arbitrar los casos con imparcialidad[121]. La Comisión Electoral General y la Agencia de Supervisión Electoral se coordinaron con el Ministerio de Comunicaciones y Tecnología de la Información para establecer una "sala de control de operaciones" desde donde se vigilaba constantemente la actividad en las redes sociales. Se encargó a la Policía Nacional que garantizara el cumplimiento de las leyes contra la desinformación y la discriminación indonesias, mientras que el gabinete del Presidente mantuvo conversaciones con organizaciones asociadas[122]. Además, la Agencia de Supervisión Electoral puso en marcha una declaración de "rechazo y lucha contra la compra de votos, las injurias, las incitaciones y los conflictos divisivos en las elecciones locales de 2018 y en las elecciones generales de 2019" que obtuvo la firma de 102 grupos

de la sociedad civil, junto con plataformas relevantes como Google, Facebook y Twitter[123].

Entre las iniciativas dirigidas por organizaciones no lucrativas, destacaron las operaciones de MAFINDO, un centro de la Comunidad Indonesia Antidifamación para hacer frente a las crisis de información falsa, que se encargó de desmentir los engaños que circulaban en las redes sociales durante las elecciones del Ejecutivo local de 2018. En 2019, la Comunidad Indonesia Antidifamación junto con 24 organizaciones de noticias gestionaron de forma similar las operaciones de CekFakta.com con financiación de Google News a fin de desmentir engaños y declaraciones falsas de los candidatos[124]. Estos asociados también desarrollaron herramientas de verificación de datos que se pusieron a disposición de la ciudadanía, como una aplicación móvil que ofrecía a las oficinas de la administración local la oportunidad de desmentir las historias falsas en tiempo real, conforme las denunciaban las personas usuarias. Entre otros proyectos figuraban las sesiones de formación sobre la lucha contra la desinformación del Centro para el Estudio de la Religión y la Democracia, dirigidas a las organizaciones de la sociedad civil; los anuncios de servicio público generados por la Comunidad Indonesia Antidifamación y la Agencia de Supervisión Electoral; y los talleres de la Fundación Internacional para Sistemas Electorales (IFES) orientados a los órganos electorales, sobre las noticias falsas y el discurso de odio basado en la identidad[125].

En el plano nacional, estas iniciativas coordinadas verificaron 821 casos de desinformación política —de los que más de la mitad estaban relacionados con las elecciones en curso—[126]. En el plano subnacional, la creación de un centro conjunto para hacer frente a las crisis de falsedades y otros proyectos locales contribuyeron a mantener la paz en zonas propensas a los conflictos, como Borneo Occidental[127]. Los esfuerzos públicos, privados y de la sociedad civil de Indonesia, constituyen un modelo de acción colectiva capaz de defender los procesos democráticos amenazados por las mentiras virales que circulan en el medio digital y la retórica violenta.


1 2 3 4 5 6 7 8
( ) €

V. LA PUBLICIDAD POLÍTICA EN LA ERA DIGITAL

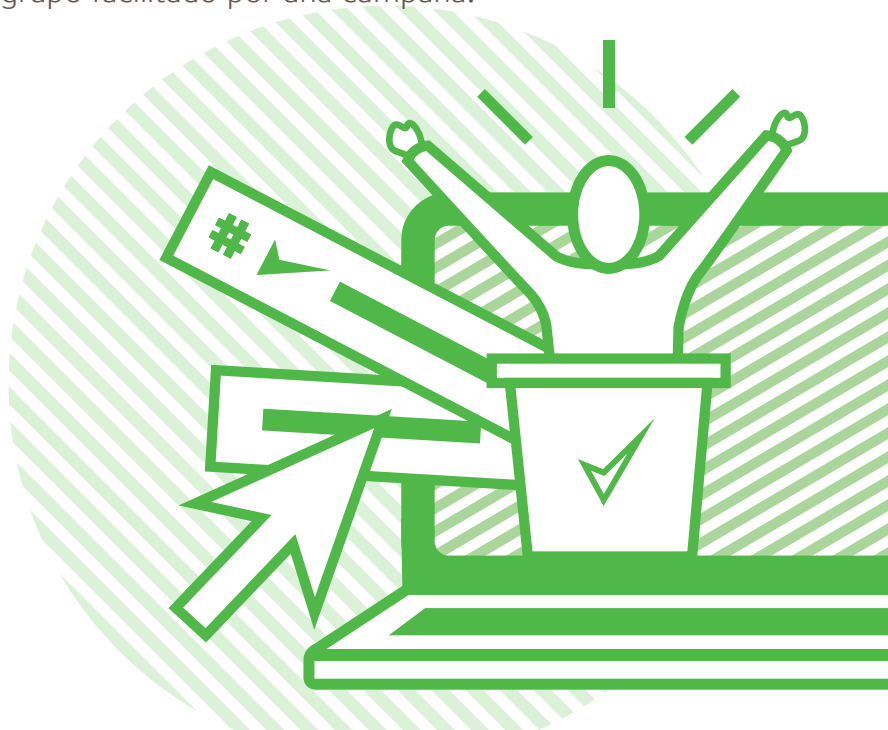
Ningún ámbito normativo referente a Internet ha recibido tanta atención en los últimos tres años como el de la reforma de la publicidad política en línea. Dada la conexión entre la publicidad en línea y la polarización, la desinformación y la injerencia extranjera en las elecciones, no cabe duda de que este aumento de la atención pública está justificado. Es más, al aceptar y promover la publicidad política, las principales plataformas de Internet se benefician de mensajes que ponen en peligro la integridad electoral y la deliberación democrática saludable, además de extenderlos y microsegmentarlos. En muchos sentidos, la publicidad en línea es una lente que permite observar el conjunto de amenazas y beneficios que Internet representa para la democracia.

La publicidad política en línea, así como Internet y las tecnologías de comunicaciones digitales en general, entrañan beneficios significativos para la democracia. Los anuncios digitales suelen ser mucho menos costosos que los anuncios de radio o televisión, lo que permite que las candidaturas con una financiación escasa transmitan sus mensajes, en particular en el plano local[128]. Además, pese a las numerosas críticas que ha recibido, la microsegmentación permite a las campañas y los grupos de interés hacer llegar los mensajes eficazmente a quienes se desea, igual que han hecho las comercializadoras durante años con la publicidad por correo postal, las llamadas telefónicas y, más tarde, el correo electrónico. Por último, Internet ha demostrado ser especialmente útil para la recaudación de fondos de pequeños donantes, ya que ha servido a las candidaturas y grupos para recaudar cantidades significativas de dinero procedentes de un gran número de donantes, y así ha "democratizado" la financiación política[129].

Sin embargo, al mismo tiempo, el ámbito de la publicidad política en línea ha demostrado ser un terreno fértil para todas las patologías democráticas asociadas con las tecnologías de comunicaciones digitales. De la misma manera que la microsegmentación puede ser útil en las iniciativas de movilización y recaudación, también permite a las campañas enviar mensajes selectivos de desmovilización o propaganda que fomente la polarización a votantes fáciles de persuadir, cuyas afinidades políticas y psicológicas es posible

identificar con cada vez más precisión gracias a las herramientas de recopilación de datos facilitadas por las plataformas de Internet y otras empresas. Asimismo, las opciones de comprobación del contenido y de aprendizaje automático permiten a anunciantes perfeccionar los mensajes que desean enviar con el fin de promover el interés en su contenido, lo que suele dar pie a que las campañas creen cientos de variaciones de un solo anuncio[130]. En consecuencia, se pueden enviar mensajes diferentes (e incluso contradictorios) a distintas personas sin que nadie más lo sepa. En este sentido, la parte negativa de la microsegmentación consiste en la creación artificial (por contraste con la autoseleccionada) de cámaras de eco en línea: las plataformas de Internet permiten a los anunciantes enviar mensajes selectivos a grupos reducidos de votantes en función de sus características demográficas, intereses, ubicación y otras variables políticas[131]. De hecho, harán también posible que se dirijan a "públicos personalizados", a partir de las listas de direcciones de correo electrónico individuales facilitadas por las campañas, y "públicos similares", los que la plataforma extrae de entre la inmensa cantidad de datos que posee mediante su correspondencia con el grupo facilitado por una campaña.

La escasa regulación de la publicidad política en línea ha abierto la puerta a la falta de transparencia en las actividades realizadas por agentes nacionales y extranjeros por igual, que han promovido mensajes falaces y polarizadores durante las campañas electorales. La intervención rusa en las elecciones presidenciales de Estados Unidos de 2016 puso de manifiesto las vulnerabilidades del sistema de



publicidad política, incluso frente a anuncios patrocinados con capital extranjero, que promovían mensajes polarizadores con la intención de influir en los resultados electorales y aprovechar la división social existente en el sistema gubernamental[132]. Con una inversión en anuncios de Facebook superior a 100.000 dólares, de los que parte se pagaron en rublos rusos, la Agencia de Investigación de Internet de la Federación de Rusia distribuyó mensajes selectivos que, si bien mencionaban ocasionalmente a los candidatos presidenciales, con frecuencia consistían en propaganda que fomentaba la polarización en torno a cuestiones sociales divisivas como la inmigración, los derechos relacionados con la posesión de armas, y la brutalidad policial por motivos raciales[133]. En ocasiones, se hacía propaganda en favor de dos opiniones enfrentadas respecto a un tema, mediante distintos anuncios, con el propósito de fomentar la división y la polarización, en lugar de persuadir a los destinatarios de las bondades de uno de los argumentos. Estos anuncios, que tendían al sensacionalismo y enmascaraban la verdadera identidad del responsable del gasto, permitieron a la Agencia de Investigación de Internet de la Federación Rusa generar audiencias a las que se podían dirigir mensajes orgánicos que se reenviaban a la red del usuario en su conjunto.

Si bien la controversia en torno a los anuncios rusos en las elecciones de 2016 no dio pie a disposiciones legislativas o normativas en Estados Unidos, sí ha forzado a las principales plataformas de Internet a poner en marcha medidas nuevas con relación a los anuncios políticos. En especial, en los dos años posteriores a las elecciones, Facebook, Google y Twitter adoptaron normas de transparencia para los anuncios políticos, y así facilitan archivos de anuncios donde personas usuarias y organismos de protección pueden consultar todos los anuncios, junto con los datos del responsable del gasto, y cierta información limitada sobre exposición y segmentación. Asimismo, con el objeto de impedir la adquisición de anuncios por parte de fuentes anónimas y extranjeras, las plataformas han adoptado sistemas de verificación conforme a los cuales empresas anunciantes políticas deben recibir tarjetas postales en su dirección declarada, y devolverlas desde la misma. De esta manera, se pretende garantizar que es posible identificar a un agente nacional como comprador genuino de un anuncio.

Aunque las plataformas de redes sociales han puesto en marcha medidas para prevenir que entidades extranjeras adquieran anuncios políticos en los Estados Unidos, éstas no han sido eficaces a la hora de prevenir que la publicidad patrocinada con capital extranjero se dirija a otras naciones[134].

Aún y cuando los responsables de las políticas de todo el mundo han presentado propuestas orientadas a aumentar el control de la publicidad política en línea, estas suelen plantear desafíos extremadamente complejos. El principal concierne a la definición de "publicidad política", es decir, ¿cómo puede la ley especificar qué tipos de temas son suficientemente "políticos" como para que los contemple la normativa en materia de publicidad política? Esto se complica aún más cuando las empresas combinan los mensajes políticos con los de consumo, como cuando un anuncio de navajas de afeitar menciona la causa contra el acoso sexual; otro de zapatillas hace referencia a la lucha de los jugadores de fútbol americano contra la brutalidad policial por motivos raciales; o uno de cerveza transmite un mensaje positivo sobre la inmigración, al explicar sus orígenes. Además, si cualquier presentación de un tema político por la que se ha pagado debe tratarse como anuncio político, esto incluirá cualquier ocasión en la que los periodistas y organizaciones de medios de comunicación paguen —como hacen con frecuencia— para promover sus reportajes en las redes sociales con el fin de que lleguen a un público más amplio. Dado que gran parte de la publicidad política que suele considerarse problemática —debido a la influencia extranjera, los mensajes polarizadores o la desinformación— se encuentra relacionada con la promoción de causas específicas, las reformas de la publicidad que no aborden esta dimensión no harán frente al "problema".

Cada plataforma ha afrontado el problema de la promoción de causas específicas de manera diferente. Twitter anunció recientemente que iba a dejar de incluir anuncios que hicieran mención de candidaturas, referéndums, o legislación pendiente, aunque seguiría permitiendo la "publicidad relacionada con causas". Google no incluye la publicidad en favor de causas en sus archivos de anuncios

políticos, pero anunció recientemente que dejará de permitir que los anunciantes empleen la segmentación basada en afiliaciones políticas, y que impedirá que en los anuncios figuren declaraciones fraudulentas de los anunciantes políticos, del mismo modo que procede ante el fraude al consumidor. Facebook proporciona el archivo de anuncios políticos más extenso, que incluye, además de anuncios de candidatos, otros que mencionan una variedad de cuestiones identificadas por la empresa a través del proyecto académico "Comparative Agendas Project" (Proyecto Comparativo de Agendas). Sin embargo, su política de "cero censura" en los anuncios políticos, que con la finalidad de preservar la libertad de expresión exime a los políticos de la verificación de datos por terceros[135], ha recibido numerosas críticas, incluso internas, como muestra la carta dirigida al *New York Times* elaborada por empleados de la empresa que argumentan que "la libertad de expresión y la expresión comprada no son lo mismo"[136].

Asimismo, las empresas y los organismos reguladores están considerando otro tipo de reformas que permitan hacer frente a las preocupaciones que genera la manipulación mediante la publicidad política. Así, algunas plataformas se han planteado establecer límites a la capacidad de segmentación con públicos personalizados, o el tamaño mínimo del público al que se dirige un anuncio político. Otras requerirían la verificación de los datos de anuncios controvertidos con el fin de asegurar que no contengan declaraciones falsas. Por otro lado, otras adaptarían los reglamentos televisivos existentes con el fin de prevenir, por ejemplo, la publicidad política durante el período inmediatamente anterior a las elecciones, cuando resulta más difícil que las campañas afronten de manera adecuada y oportuna la desinformación para marcar la diferencia. En muchos de estos ámbitos, las propias plataformas han pedido orientación legislativa, ya que han llegado a reconocer que estas decisiones son simple y llanamente demasiado importantes y centrales para la democracia como para que las empresas multinacionales, cuyo objetivo es conseguir el máximo beneficio, dicten las reglas.

CONSECUENCIAS PARA LA ACCIÓN

La publicidad política digital responsable requiere que los partidos políticos, las plataformas de redes sociales y las autoridades públicas competentes actúen. En primer lugar, los políticos, partidos políticos y candidatos deben responsabilizarse del uso de la publicidad digital, de manera que respete la integridad electoral. El modo en que estos utilizan las nuevas tecnologías de publicidad digital para hacer campaña puede marcar el rumbo de unas elecciones, y ofrecer a los ciudadanos un alto grado de seguridad, confianza e información, o socavar la integridad electoral mediante su participación en prácticas de campaña engañosas que hacen hincapié en los rumores, las conspiraciones, la desinformación y la manipulación de los medios de comunicación. Ya existen ejemplos de políticos que se rigen por códigos de conducta y mejores prácticas con el fin de promover un entorno saludable en sus campañas políticas **[Recuadro 7]**. La integridad electoral en la era digital requiere normas éticas más rigurosas que gobiernen el modo en que los políticos, los partidos y los candidatos utilizan los medios sociales y la publicidad digital.

Refrendamos el llamamiento de la Comisión Transatlántica sobre Integridad Electoral a que los candidatos, partidos y grupos políticos firmen compromisos de rechazo de las prácticas engañosas de campaña digital. Dichas prácticas incluyen el uso de datos o materiales robados, la utilización de imágenes manipuladas —como la manipulación de imágenes, vídeos y audios; la creación de estos empleando la inteligencia artificial; y la difusión de desnudos generados digitalmente—, la producción, uso o difusión de materiales falsificados, y la confabulación con gobiernos extranjeros y sus agentes que tratan de manipular las elecciones.

RECUADRO 7

El Acuerdo de Abuja (Nigeria) sobre la conducta electoral, 2015

En el período previo a las elecciones generales de Nigeria de 2015, existía aprensión entre muchos nigerianos por la posible repetición de lo acontecido en las elecciones de 2011, marcadas por la violencia preelectoral a gran escala que provocó más de 800 muertos y miles de desplazados internos[137]. Kofi Annan, alarmado por la posibilidad de una catástrofe electoral, visitó el país e instó a los candidatos presidenciales a que firmaran un acuerdo de paz mediante el cual se comprometían a dirigir campañas limpias y objetivas. En enero de 2015 en Abuja, con Annan como testigo, los candidatos se comprometieron a abstenerse de realizar una campaña negativa que pudiera incitar a la violencia por razones religiosas, tribales o étnicas[138]. Numerosas organizaciones nacionales pusieron en marcha el acuerdo, incluidos líderes religiosos cristianos y musulmanes, con la asistencia de varias organizaciones no gubernamentales[139]. El Acuerdo instaba a la creación de un Comité Nacional de la Paz que se encargaría de vigilar el cumplimiento del acuerdo[140].

El Acuerdo de Abuja fue todo un éxito. En marzo de 2015, a solo dos días de las elecciones presidenciales, los dos candidatos principales renovaron el Acuerdo como símbolo de la unidad, estabilidad y seguridad nacional antes del día de las elecciones[141]. El Acuerdo se adoptó rápidamente como modelo en otros procesos electorales, como en el período previo a las elecciones de octubre de 2019 en Mozambique[142]. La mayoría de los representantes estatales de Nigeria han firmado también variaciones del Acuerdo[143]. Durante el ciclo de las elecciones generales de 2019, los líderes de los partidos nigerianos firmaron otro acuerdo con el mismo espíritu[144]. El legado del Acuerdo de Abuja demuestra la posible eficacia de los compromisos de las campañas con la conducta política cívica y no violenta.

En segundo lugar, las principales empresas de redes sociales han tomado medidas para hacer frente a algunos de los nuevos desafíos digitales en materia de publicidad política. No obstante, creemos que se pueden hacer mayores esfuerzos en aras de la integridad electoral. En especial, todas las plataformas podrían tomar medidas adicionales para mejorar la transparencia de la publicidad política —como la publicación de más datos sobre la microsegmentación y la revelación de la identidad de quienes compran la publicidad—, además de ofrecer a los usuarios mayor control sobre el tipo de anuncios que se les ofrecen. Asimismo, las plataformas podrían ayudar a reforzar las normas positivas en las campañas políticas obligando a los políticos, partidos y personas candidatas que adquieren anuncios a que suscriban el compromiso de evitar las prácticas de campaña engañosas, y obligando a sus anunciantes políticos a respetar tales compromisos. Todas estas medidas pueden favorecer la integridad electoral.

Las plataformas deben ofrecer mayor transparencia en torno a los anuncios políticos.

- Las plataformas deben ofrecer a los usuarios la opción de incluir o excluir la publicidad política.

- Las plataformas solo deben permitir la adquisición de anuncios a aquellas candidaturas, partidos y grupos que se hayan comprometido a evitar las prácticas de campaña engañosas. Posteriormente, tales compromisos deben convertirse en las normas de funcionamiento de las plataformas para decidir si aceptan un anuncio dado.

- A fin de evitar el encubrimiento de las fuentes de financiación tras etiquetas organizacionales engañosas, las plataformas deben requerir que se publique la identidad de las personas que financian los anuncios políticos.

Por último, es preciso que las autoridades públicas competentes acepten su responsabilidad en la protección de la integridad electoral. Aún más importante es la necesidad de adaptar a la era digital las leyes y reglamentos que rigen la publicidad y las campañas políticas. En especial, la definición de la publicidad política debe ser una cuestión jurídica, y no dejarse en manos de empresas cuyo objetivo es obtener el máximo beneficio. Las autoridades públicas competentes deben especificar también el tamaño mínimo del público para la microsegmentación de anuncios políticos, y considerar el reconocimiento en la legislación de un período de reflexión para los anuncios políticos digitales, de manera similar a las leyes de radiodifusión actuales de algunos países. Pese a que las plataformas han dado pasos significativos para mejorar la transparencia de los anuncios políticos, es necesario seguir trabajando para promover un entorno que fomente la integridad electoral. Los gobiernos deben tomar medidas con el propósito de obligar a las empresas de medios sociales a que hagan públicos los datos relativos a la publicidad política; por ejemplo, requerir que las plataformas publiquen la información relativa a la identidad de los anunciantes, los criterios de segmentación, las sumas gastadas, y el trabajo creativo real de los anuncios.

Los países deben adaptar su reglamento de publicidad política al entorno en línea. Las autoridades públicas competentes deben:

- Definir por la vía legislativa, qué se considera un anuncio político.
- Obligar a las plataformas de redes sociales a publicar toda la información relacionada con la adquisición de un anuncio, incluida la identidad real del anunciante, la suma pagada, el criterio de segmentación, y el verdadero trabajo creativo del anuncio.
- Especificar en la legislación el tamaño mínimo del segmento de público para un anuncio.
- Establecer jurídicamente un período de reflexión mínimo para los anuncios políticos digitales, de 48 horas antes de unas elecciones.

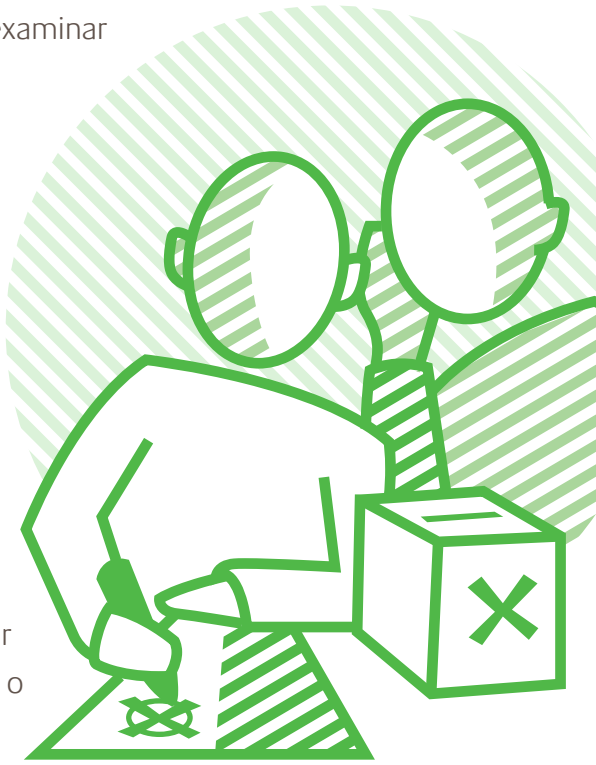
VI. LA PROTECCIÓN DE LAS ELECCIONES FRENTE A LA INJERENCIA EXTRANJERA

Pese a que Internet y las redes sociales tienen numerosos efectos positivos en la democracia y las elecciones —entre otros, la promoción de la libertad de expresión, las oportunidades de movilización política, y la democratización de la información—, su potencial uso indebido queda más patente que nunca cuando se analiza desde el punto de vista de las operaciones de injerencia extranjera. A lo largo del último decenio, agentes estatales y no estatales se han aprovechado de Internet para poner en práctica sus agendas políticas, económicas y militares, y han combinado estratégicamente las operaciones militares tradicionales con los ciberataques y las campañas de propaganda en línea. Como es posible explotar la naturaleza abierta, anónima y sin fronteras de las tecnologías digitales, las redes sociales han brindado oportunidades nuevas para que agentes mal intencionados se inmiscuyan en el plano transnacional. La integridad electoral depende de la soberanía de las elecciones, y los agentes externos no deberían poder determinar su resultado.

Hasta la fecha, el ejemplo más prolífico de intrusión extranjera ha sido la injerencia rusa en las elecciones presidenciales de los Estados Unidos de 2016. Mediante la combinación de técnicas de piratería tradicionales, con campañas coordinadas digitalmente en toda una variedad de medios nuevos y tradicionales, agentes rusos intentaron influir en el público estadounidense y repercutir en el resultado electoral. Se filtraron estratégicamente datos robados con la intención de dañar la candidatura presidencial de Hillary Clinton[145]. Medios informativos controlados por la Federación Rusa —como Russia Today y Sputnik— difundieron historias conspirativas y avivaron la narrativa de corrupción en contra de Hillary Clinton en canales de televisión y YouTube. Mediante cuentas falsas y automatizadas de la Agencia Rusa de Investigación de Internet, se extendieron estos mensajes en Facebook, Twitter e Instagram. Se dirigieron a las comunidades de votantes anuncios políticos —diseñados con el objeto de polarizar al público en torno

a cuestiones políticas sumamente delicadas— con el fin de fomentar la división y la desconfianza entre la población estadounidense. Y las publicaciones, las páginas y los grupos se hicieron considerablemente virales de manera gratuita, con lo que se llegó a más de 126 millones de estadounidenses en el período previo a la votación de 2016[146].

Aunque la injerencia rusa durante las elecciones estadounidenses de 2016 ofrezca uno de los ejemplos más prolíficos —sobre todo si se tienen en cuenta la escala y la sofisticación de la campaña—, Estados Unidos no ha sido el único país afectado por la intrusión rusa. Se han descubierto huellas de campañas de desinformación patrocinadas por Rusia en numerosas partes del mundo, como Ucrania, el Reino Unido y en el continente africano[147]. Lo más inquietante es que el modelo ruso de injerencia electoral, centrado en la acción de un Estado-Nación encaminada a desestabilizar a un adversario, ha sido adoptado por otros países que aspiran a ejercer influencia geopolítica a través de las redes sociales. No hay más que examinar la reciente campaña de desinformación de China contra los manifestantes de Hong Kong, que calificaba a los activistas políticos de violentos y afirmaba que no contaban con gran apoyo[148], o las operaciones de influencia de la República Islámica del Irán, que promueven la narrativa anti-saudí y anti-israelí, e instan a apoyar las políticas de Estados Unidos favorables a Irán[149].



Uno de los desafíos de la lucha contra las operaciones de influencia extranjera, deriva de la creciente dificultad para distinguir entre la actividades normales de campaña desarrolladas por agentes políticos nacionales oficiales, y las operaciones informativas antidemocráticas dirigidas por gobiernos extranjeros, entidades comerciales sospechosas o

grupos nacionales. Los políticos y partidos populistas han utilizado las mismas herramientas y estrategias que los agentes extranjeros para impulsar la retórica ultranacionalista y antinmigrante en los debates políticos generales. Los grupos de presión han empleado las redes sociales con el objetivo de exponer a la ciudadanía de países extranjeros a mensajes partidistas. Un ejemplo de esto es la actividad de grupos provida de los Estados Unidos, que dirigieron publicidad política a personas irlandesas durante el período previo al referéndum de Irlanda de 2018, sobre el tema del aborto[150]. A menudo, estos esfuerzos y actividades se solapan, lo que difumina los límites tradicionales entre la actividad política extranjera y nacional, los gobiernos y las organizaciones no gubernamentales, y las operaciones de información y las actividades de campaña que se consideran admisibles.

UNA INDUSTRIA TRANSNACIONAL EMERGENTE DE MANIPULACIÓN ELECTORAL

El libro de tácticas en materia de injerencia, también ha resultado lucrativo para los agentes privados y las empresas de comunicaciones estratégicas, que venden las diversas opciones de injerencia electoral a los interesados en sus servicios. El escándalo en torno a Cambridge Analytica —que adquirió notoriedad por su uso indebido de los datos de Facebook a fin de dirigir propaganda a los votantes durante las elecciones estadounidenses de 2016—, es uno de los ejemplos más escandalosos que resaltan cómo se ha profesionalizado la manipulación electoral[151]. A través de la explotación de datos privados de las redes sociales y su infraestructura, Cambridge Analytica —y su empresa matriz, Strategic Communications Laboratories (SCL Group)— elaboró, dirigió, y adaptó mensajes de persuasión y desmovilización para intentar influir en los resultados electorales de países de todo el mundo, como Nigeria, Sri Lanka, Kenya, Filipinas, Trinidad y Tabago, y el Reino Unido[152]. Aunque la eficacia de las técnicas de minería de datos y “elaboración

de perfiles psicográficos" de Cambridge Analytica se ha exagerado significativamente[153], este caso pone de relieve el fenómeno más general de la profesionalización de la manipulación electoral.

En la actualidad, existe una variedad de empresas, consultorías, agencias de comunicaciones políticas y empresas de mercadotecnia digital que se valen de las herramientas del sector de la mercadotecnia para influir en los votantes[154]. Estas empresas se encuentran presentes en todo el mundo y han trabajado con los políticos y los gobiernos para difundir desinformación y propaganda, así como hacer llegar a los votantes mensajes encaminados a inhibir su voto[155]. En algunos casos, estas empresas operan a escala internacional con el fin de ocultar la identidad real de la persona u organización que se esconde tras una campaña cuyo objetivo es ejercer influencia[156], así como para aprovechar la mano de obra digital barata de países como la India[157] o Filipinas[158], donde ha surgido una industria lucrativa de "granjas de troles".

LA PROTECCIÓN DE LA INFRAESTRUCTURA ELECTORAL

Todos los ciudadanos tienen el derecho a que su voto se cuente de manera imparcial y exacta, y la confianza ciudadana en el recuento de votos goza de una importancia crucial para la integridad electoral. No obstante, la integridad electoral es en gran medida una caja negra que se mantiene gracias a la fe de los votantes, en que están registrados jurídicamente, su voto se ha contabilizado, y los resultados anunciados por las autoridades electorales son exactos.

Además de los efectos tenues y sutiles que la propaganda y la desinformación pueden tener en las elecciones, es importante reconocer las sustanciales preocupaciones en materia de ciberseguridad relacionadas con las tecnologías electorales electrónicas.

La protección del *hardware* y *software* informáticos de registro de votantes y emisión de votos es esencial para la integridad de las elecciones. Al margen de las tecnologías electrónicas electorales, existe un ecosistema vasto y descentralizado de tecnologías de apoyo a las elecciones, en el que se incluyen los sistemas de registro de votantes en línea, los de recuento de votos, y los de auditoría. Todas estas tecnologías son sensibles a ataques digitales, así como a errores internos, que pueden erosionar la confianza del votante y afectar a la integridad de las elecciones.

La piratería del *hardware* y el *software* electoral puede tener como objetivo alterar los resultados, manipular las listas de votantes o simplemente socavar la confianza ciudadana en las elecciones. Los motivos de dicha piratería pueden reducirse al deseo de un gobierno extranjero o un agente nacional de asegurarse un resultado favorable. La piratería tan solo representa una de las herramientas posibles de manipulación de las tecnologías electrónicas electorales. Por ejemplo, en las elecciones de 2014 de Mozambique, el Gobierno suprimió la inscripción electoral biométrica en las zonas controladas por la oposición "mediante el envío de equipo inadecuado y personal sin capacitación suficiente"[159]. Más allá de la injerencia en favor de una candidatura en particular, los gobiernos extranjeros pueden tener un interés general en sembrar tensiones en el ámbito nacional, provocar caos, minar la legitimidad, generar desconfianza y, de ese modo, debilitar el país objetivo. Cuando surgen dudas sobre la seguridad de las tecnologías electrónicas electorales, es muy fácil que los agentes políticos descontentos con los resultados, achaquen la derrota en las urnas a la manipulación del *hardware* y el *software* de votación, y socavar aún más la confianza ciudadana en el proceso y el resultado.

Por otra parte, la seguridad de las tecnologías electrónicas electorales no es solo una cuestión técnica, y los propios funcionarios electorales pueden poner en peligro dichas tecnologías —de manera intencionada o no—[160]. Como las personas "participan estrechamente en todas las operaciones electorales, no cabe duda de que es posible explotar las debilidades humanas"[161]. La resiliencia de la infraestructura electoral dependerá de la protección de los sistemas técnicos, así como de garantizar que las personas presentes en todas las partes del ecosistema de las tecnologías electrónicas electorales poseen formación en las mejores prácticas de ciberseguridad. Cabe resaltar, una vez más, el papel esencial de los órganos electorales profesionales, competentes e independientes, a la hora de proteger la integridad electoral en la era digital.

CONSECUENCIAS PARA LA ACCIÓN

Cuando los agentes estatales interfieren en elecciones extranjeras, existe una serie de recursos jurídicos con arreglo al derecho internacional. El Artículo 2 de la Carta de las Naciones Unidas garantiza la integridad territorial y política de los Estados, por lo que las campañas de injerencia extranjera promovidas por agentes estatales atentan contra esta garantía. Los gobiernos pueden impulsar este recurso mediante la declaración del *hardware* y el *software* electoral como infraestructura vital, y la negociación de una norma internacional contra los ciberataques a infraestructuras vitales.

Los gobiernos democráticos deben considerar las tecnologías electrónicas electorales como infraestructura vital, y apoyar la norma refrendada por el Grupo de los 20 conforme a la cual los "Estado[s] no deben llevar a cabo ni apoyar conscientemente actividades en materia de tecnología de la información y las comunicaciones [...] que dañen intencionalmente la infraestructura vital".

No obstante, constituye un desafío mayor cómo proteger la asistencia extranjera legítima destinada a promover la democracia y la integridad electoral, y distinguirla de la injerencia extranjera ilegítima en unas elecciones. Con demasiada frecuencia, los defensores de los actos recientes de injerencia extranjera en elecciones democráticas afirman que las acciones rusas no son distintas de los esfuerzos llevados a cabo por las democracias occidentales cuando apoyan el desarrollo de partidos políticos en África, o respaldan a las organizaciones de la sociedad civil que abogan por la rendición de cuentas de los gobiernos autoritarios. La mejor manera de refutar estos argumentos basados en una equivalencia falaz es que las democracias detallen qué es y qué no es apoyo transnacional legítimo a la democracia.

Los gobiernos democráticos deben reunirse para establecer un convenio internacional sobre el papel de los gobiernos extranjeros y sus agentes en las elecciones de otros países; más específicamente, deben desarrollar normas internacionales que distingan la asistencia transfronteriza legítima de las intervenciones ilícitas o ilegales.

Al margen de la injerencia extranjera por parte de agentes estatales, no existen normas o reglamentos rectores sobre la industria emergente de la manipulación electoral. A pesar de los escándalos y sus prácticas contrarias a la ética, empresas como Cambridge Analytica han podido cambiarse el nombre y seguir operando. Se necesita regulación gubernamental, mejores prácticas y códigos de conducta dirigidos a consultorías políticas y las empresas de comunicación estratégica. Dos asociaciones profesionales voluntarias, la Asociación Internacional de Consultores Políticos y la Asociación Americana de Consultores Políticos, han elaborado códigos de conducta que podrían servir como foro para el diálogo entre el sector de la consultoría

electoral, los gobiernos, y la comunidad del ámbito de la integridad electoral en su conjunto, para crear y aplicar normas transnacionales obligatorias de consultoría ética de campaña.

La comunidad del ámbito de la integridad electoral debe crear normas y estándares para las consultorías de campañas políticas transnacionales, incluidas las empresas de relaciones públicas y comunicaciones estratégicas, y comercializadoras digitales. La regulación gubernamental debe desarrollar procedimientos para la certificación de estas consultorías e impedir que una empresa que infrinja las normas, reglas y estándares relativos a la consultoría de campañas continúe trabajando en procesos electorales.

Las tecnologías electorales electrónicas desempeñan un papel central en casi todas las facetas del proceso electoral y, en consecuencia, la solidez de la ciberseguridad constituye un elemento esencial para garantizar elecciones íntegras. No obstante, la protección de este tipo de tecnologías plantea desafíos. Uno de los principales obstáculos a la hora de proteger las elecciones democráticas de la piratería es la falta de transparencia y cooperación entre los principales proveedores de tecnologías electorales electrónicas, que se han adaptado con lentitud a las amenazas digitales contra la integridad electoral. Es posible que los funcionarios electorales no tengan el conocimiento técnico necesario para garantizar los sistemas que supervisan. A veces, los órganos electorales están más preocupados por que las advertencias sobre la susceptibilidad de sus sistemas a la piratería deterioren la confianza de los votantes que por las propias amenazas de injerencia externa[162]. En algunos países, la corrupción existente en el proceso de adquisición de tecnologías electrónicas electorales se debe a que los proveedores están dispuestos a ofrecer sobornos a los funcionarios para que adquieran equipo caro que no es seguro ni apropiado para el nivel de desarrollo del país[163].

La comunidad del ámbito de la integridad electoral debe apoyar a los órganos electorales en la adquisición de conocimientos especializados en mejores prácticas de ciberseguridad.

Es posible que ciertos órganos electorales requieran asistencia técnica a corto plazo para hacer frente a las amenazas contra la integridad electoral que plantea la injerencia extranjera en elecciones, la piratería y los discursos de odio, que conducen a la violencia relacionada con las elecciones. En tales casos, la asistencia técnica internacional para ayudar a estos órganos a defender su proceso electoral debe estar disponible en el momento en que se solicite. Con el fin de garantizar que dicha asistencia se brinde con apremio, se recomienda el desarrollo de equipos permanentes de ciberseguridad electoral que puedan desplegarse inmediatamente bajo petición. Dichos equipos podrían formar parte de organizaciones internacionales existentes, como la División de Asistencia Electoral de las Naciones Unidas, organizaciones regionales o una nueva institución internacional. Asimismo, deben poder emplear turnos rotativos en la ocupación de puestos técnicos, a fin de garantizar la aplicación de las mejores prácticas gubernamentales en el plano digital.

Pese a su importancia crucial para la integridad electoral y la confianza pública en los resultados electorales, la industria de las tecnologías electrónicas electorales no cuenta con regulación a escala mundial. Ya son varios los gobiernos y las empresas tecnológicas privadas con lazos estrechos con sus respectivos gobiernos que se han convertido en proveedores de equipo servicios de apoyo electoral. No existen garantías de que tales proveedores no se transformarán en herramientas de la política extranjera, en lugar de actuar como proveedores independientes de servicios electorales. Cada vez es más común que los gobiernos autoritarios comercialicen tecnologías de doble uso, capaces de facilitar servicios de registro e identificación de votantes, pero con potencial de emplearse para vigilar a los ciudadanos y los oponentes.

La industria de la tecnología electoral mundial tiene la obligación de colaborar en las iniciativas de establecimiento de normas mundiales

con miras a proteger la información digital, el escrutinio y la transmisión de resultados, así como el equipo de *hardware* y *software*, contra las intervenciones nacionales o extranjeras, la piratería, la manipulación o las injerencias. Esto beneficiaría no solo a las democracias de todo el mundo, sino también a las empresas de tecnologías electorales que se erijan como líderes en el mantenimiento de la integridad electoral.

Los proveedores de equipos y servicios electorales deben comprometerse a cumplir un código de conducta, con el fin de garantizar que sus productos son seguros y sus prácticas comerciales protegen los derechos, la privacidad y los datos de la ciudadanía en sus países clientes, y adoptar prácticas de adquisición honestas y transparentes. A su vez, la comunidad internacional del sector de la integridad electoral se debe comprometer a condicionar la asistencia electoral a los países, a la firma y el cumplimiento del código por parte de los proveedores. Una iniciativa de múltiples partes interesadas, en la que participe la comunidad de la integridad electoral, la Red Global de Monitores Electorales Nacionales y los asociados internacionales deben elaborar dicho código de conducta.

VII. RESUMEN DE RECOMENDACIONES

La defensa de la integridad electoral contra el uso indebido y el abuso de las redes sociales dependerá de las decisiones y el comportamiento de las principales empresas y plataformas tecnológicas, así como de los gobiernos, los políticos, los medios tradicionales, los órganos electorales y la ciudadanía. Con el fin de proteger la integridad electoral en la era digital, necesitaremos fortalecer las capacidades de los defensores de dicha integridad y elaborar normas compartidas sobre el uso adecuado de las tecnologías digitales en las elecciones. Las plataformas tecnológicas y las autoridades públicas deben adoptar medidas encaminadas a reforzar la integridad electoral.

EL DESARROLLO DE LAS CAPACIDADES PROPIAS

Recomendación núm. 1.

Se debe prestar más atención y destinar más recursos a la promoción de la integridad electoral. Las autoridades públicas, las organizaciones internacionales, las fundaciones filantrópicas y la sociedad civil deben invertir en el desarrollo de habilidades tecnológicas y capacidad digital, en los esfuerzos mediáticos y en los órganos de gestión electoral que protejan y promuevan la integridad electoral. Todas las partes interesadas deben cooperar, colaborar y compartir con rapidez la información relacionada con las amenazas a la integridad electoral. Estas actuaciones deben incluir:

- La creación de un índice de vulnerabilidad electoral que mida qué elecciones requieren un seguimiento estricto de las posibles injerencias electorales, el comportamiento falaz coordinado en línea y la desinformación posibles.

- El desarrollo de las capacidades propias de las asociaciones nacionales, cuyo objetivo consiste en defender la integridad de las elecciones frente a la instrumentalización de la desinformación, y apoyar la mejora de las prácticas de evaluación e intercambio de información.
- La financiación de las organizaciones de la sociedad civil que luchan contra el discurso de odio, el acoso selectivo y la incitación a la violencia, especialmente en el período previo a las elecciones.
- La ayuda dirigida a los órganos electorales con miras a adquirir conocimientos especializados relativos a las mejores prácticas de ciberseguridad.
- El apoyo a las democracias con vistas a desarrollar programas de tecnología cívica a través de la formación en codificación, especialmente para las mujeres y las minorías, y mediante la incorporación de personal con habilidades técnicas en los equipos gubernamentales.

Recomendación núm. 2.

Algunos órganos electorales pueden necesitar asistencia técnica a corto plazo para hacer frente a las amenazas a la integridad electoral, causadas por la injerencia extranjera en las elecciones, la piratería y los discursos de odio, que conducen a la violencia relacionada con las elecciones. En tales casos, la asistencia técnica internacional para ayudar a estos órganos a defender su proceso electoral debe estar disponible en el momento en que se solicite. Con el fin de garantizar que dicha asistencia se brinde con apremio, se recomienda el desarrollo de equipos permanentes de ciberseguridad electoral que puedan desplegarse inmediatamente bajo petición. Dichos equipos podrían formar parte de organizaciones internacionales existentes, como la División de Asistencia Electoral de las Naciones Unidas, organizaciones regionales o una nueva institución internacional. Asimismo, deben poder emplear turnos rotativos en la ocupación de puestos técnicos a fin de garantizar la aplicación de las mejores prácticas gubernamentales en el plano digital.

LA CREACIÓN DE NORMAS

Recomendación núm. 3.

Refrendamos el llamado de la Comisión Transatlántica sobre la Integridad de las Elecciones a que las personas candidatas, partidos y grupos políticos firmen compromisos de rechazo de las prácticas engañosas de campaña digital. Dichas prácticas incluyen el uso de datos o materiales robados, la utilización de imágenes manipuladas —como la manipulación de imágenes, vídeos y audios; la creación de éstos empleando la inteligencia artificial; y la difusión de desnudos generados digitalmente—, la producción, uso o difusión de materiales falsificados, y la confabulación con gobiernos extranjeros y sus agentes que tratan de manipular las elecciones.

Recomendación núm. 4.

Los gobiernos democráticos deben ponerse de acuerdo y establecer una convención internacional sobre el papel de los gobiernos extranjeros y sus agentes en las elecciones de otros países. En especial, deben desarrollar normas internacionales que distingan la asistencia transfronteriza legítima de las intervenciones ilícitas o ilegales.

Recomendación núm. 5.

Los gobiernos democráticos deben considerar las tecnologías electrónicas electorales como infraestructura vital, y apoyar la norma refrendada por el Grupo de los 20 conforme a la cual los "Estado[s] no deben llevar a cabo ni apoyar conscientemente actividades en materia de tecnología de la información y las comunicaciones [...] que dañen intencionalmente la infraestructura vital".

Recomendación núm. 6.

Los proveedores de equipos y servicios electorales deben comprometerse a cumplir un código de conducta, con el fin de garantizar que sus productos son seguros y sus prácticas comerciales protegen los derechos, la privacidad y los datos de la ciudadanía en sus países

clientes; y adoptar prácticas de adquisición honestas y transparentes. A su vez, la comunidad internacional del sector de la integridad electoral se debe comprometer a condicionar la asistencia electoral a los países, a la firma y el cumplimiento del código por parte de los proveedores. Una iniciativa de múltiples partes interesadas, en la que participe como mínimo la comunidad de la integridad electoral, la Red Global de Monitores Electorales Nacionales y los asociados internacionales deben elaborar dicho código de conducta.

Recomendación núm. 7.

La comunidad que trabaja en el ámbito de la integridad electoral debe crear normas y estándares para las consultorías de campañas políticas transnacionales, incluidas las empresas de relaciones públicas y comunicaciones estratégicas, y las comercializadoras digitales. La regulación gubernamental debe desarrollar procedimientos para la certificación de estas consultorías y a fin de impedir que una empresa que infrinja las normas, reglas y estándares relativos a la consultoría de campañas continúe trabajando en procesos electorales.

LA ACTUACIÓN DE LAS AUTORIDADES PÚBLICAS

Recomendación núm. 8.

Los países deben adaptar su reglamento de publicidad política al entorno en línea. Las autoridades públicas competentes deben:

- Definir por vía legislativa qué se considera un anuncio político.

- Obligar a las plataformas de redes sociales a publicar toda la información relacionada con la adquisición de un anuncio, incluida la identidad real del anunciante, la suma pagada, el criterio de segmentación, y el verdadero trabajo creativo del anuncio.

- Especificar en la legislación el tamaño mínimo del segmento de público para un anuncio.

- Establecer jurídicamente un período de reflexión mínimo para los anuncios políticos digitales de 48 horas antes de unas elecciones.

Recomendación núm. 9.

Las autoridades públicas deben obligar a las principales plataformas de Internet a proporcionar a las partes independientes datos significativos sobre el impacto que las redes sociales tienen en la democracia. En concreto, las plataformas deben:

- Compartir datos seguros que protejan la privacidad, con instituciones académicas certificadas para el estudio de cuestiones como el análisis de algoritmos en materia de tendencias extremistas; la comprensión del efecto de las redes sociales en la polarización política y el consumo de información; y el esclarecimiento de la relación entre el discurso de odio en línea y la violencia física.

- Actualizar los informes de transparencia con miras a hacer públicos los datos relativos al número de denuncias de discurso de odio y abusos en línea. Se deben incluir datos sobre los casos de abuso selectivo (por razón de género, raza, orientación sexual o religión) y la frecuencia con que distintas comunidades se ven afectadas.

- Identificar las cuentas automatizadas. Cuando las plataformas no identifiquen correctamente las cuentas automatizadas (p. ej., un bot), deben enfrentarse a sanciones económicas.

Recomendación núm. 10.

Las autoridades públicas deben promover los programas de alfabetización digital y mediática en las escuelas y la programación de interés público entre la población en general.

LA ACTUACIÓN DE LAS PLATAFORMAS

Recomendación núm. 11.

Las plataformas deben ofrecer mayor transparencia en torno a los anuncios políticos.

- Las plataformas deben ofrecer a las personas usuarias la opción de incluir o excluir la publicidad política.

- Las plataformas solo deben permitir la adquisición de anuncios a aquellas personas candidatas, partidos y grupos que se hayan comprometido a evitar las prácticas de campaña engañosas. Posteriormente, tales compromisos deben convertirse en las normas de funcionamiento de las plataformas para decidir si aceptan un anuncio dado.

- A fin de evitar el encubrimiento de las fuentes de financiación tras etiquetas de organizacionales engañosas, las plataformas deben requerir que se publique la identidad de las personas que financian los anuncios políticos.

Recomendación núm. 12.

Las plataformas de redes sociales deben desarrollar sistemas de alerta temprana que permitan detectar la desinformación electoral, la injerencia extranjera, los delitos de odio, las amenazas contra las mujeres, la violencia y la supresión de los votantes.

- Las plataformas deben emplear más expertos que dominen los idiomas locales y tengan competencia cultural en el lugar en donde operan.

- Puesto que cuando la comunicación ya se ha hecho viral es demasiado tarde para tomar medidas, los sistemas de alerta temprana deben comenzar a aplicar la revisión por parte de personas físicas de las cuentas y las publicaciones que

representan una posible amenaza para las elecciones. Una persona física ha de encargarse de la revisión y del control del contenido que, en mayor o menor medida, se hace viral.

Recomendación núm. 13.

Las plataformas de redes sociales deben crear una coalición con el propósito de afrontar las amenazas digitales a la democracia y la integridad de los procesos electorales, de manera similar a la colaboración mantenida en el ámbito de la lucha contra el terrorismo y la explotación infantil. Los miembros de las coaliciones deben reunirse con regularidad y crear estrategias para múltiples plataformas a fin de detectar y limitar el alcance de la instrumentalización de la desinformación.

AGRADECIMIENTOS

Queremos expresar nuestro más sincero agradecimiento a las personas e instituciones que han contribuido al trabajo de la Comisión a lo largo de nuestras deliberaciones.

Laura Jakli, estudiante de doctorado de la Universidad de California Berkeley, se encargó de la dirección de un pequeño equipo de investigación en el Centro sobre Democracia, Desarrollo y Estado de Derecho de la Universidad de Stanford que ofreció apoyo a Stephen Stedman. Sus integrantes eran: Sylvie Ashford, Carolyn Chun, Yingjie Fan y Whitney McIntosh. Laura Jakli y Samantha Bradshaw, estudiante de doctorado del Oxford Internet Institute, contribuyeron

sustancialmente a la redacción y revisión del informe. Young Lee y Eloise Duvillier ofrecieron apoyo presupuestario y administrativo en la Universidad de Stanford.

Declan O'Brien, Sebastian Brack, Li Ling Low, y Stephanie Lewis de la Fundación Kofi Annan brindaron el apoyo organizativo necesario para el funcionamiento de la Comisión. Bijan Farnoudi y Genna Ingold se encargaron de las comunicaciones y la estrategia de divulgación.

Asimismo, varios académicos y profesionales ofrecieron sus ideas a la Comisión: Tanja Bosch, Pablo Boczkowski, Michelle Brown, Chipo Dendere, Katherine Ellena, Jonas Kaiser, Daphne Keller, Admire Mare, Mora Matassi, Pat Merloe, Eugenia Mitchelstein, Vasu Mohan, Joyojeet Pal y Erica Shein.

El Grupo Central de la Iniciativa de Integridad Electoral de la Fundación Kofi Annan actuó como grupo de consulta en materia de ideas y recomendaciones.

La Fundación Kofi Annan desea expresar también su reconocimiento al equilibrado y diverso grupo de asociados en la financiación que ha respaldado la labor de la Comisión: la Cancillería Federal de Austria, la Open Society Foundation, la Fundación pro Naciones Unidas, William H. Draper III, Facebook y Twitter.

Esta combinación de agentes de la industria, gobiernos, fundaciones y particulares promovió la participación constructiva sin comprometer la independencia de la Comisión.

ACERCA DE LA FUNDACIÓN KOFI ANNAN

La Fundación Kofi Annan es una organización independiente sin ánimo de lucro que dedica su labor a la promoción de una mejor gobernanza mundial a escala mundial y el fortalecimiento de las capacidades individuales y nacionales a fin de lograr un mundo más justo y pacífico.

La Fundación moviliza voluntad política con vistas a superar las amenazas para la paz, el desarrollo y los derechos humanos. En la mayoría de los casos, las pruebas y los conocimientos especializados necesarios para resolver los problemas apremiantes como la pobreza, el conflicto armado y la mala gobernanza ya existen. Lo que nos impide avanzar es la falta de liderazgo o voluntad política para identificar las soluciones y ponerlas en práctica. La Fundación moviliza a personas dotadas, por su posición, de la influencia y el liderazgo necesarios para afrontar los problemas más urgentes del mundo.

BIBLIOGRAFÍA

1 Nathaniel Persily. "The Internet's Challenge to Democracy: Framing the Problem and Assessing Reforms", informe para la Comisión Kofi Annan sobre Elecciones y Democracia en la Era Digital, 2019. **2** Pablo J. Boczkowski, Eugenia Mitchelstein y Mora Matassi, "Social Media and Democracy in Latin America", informe para la Comisión Kofi Annan sobre Elecciones y Democracia en la Era Digital, 2019. **3** Boczkowski, Mitchelstein y Matassi, "Social Media and Democracy in Latin America". Véase también Tanja Bosch, Chipo Dendere y Admire Mare, "The Effect of Social Media on Democracy and Elections in Africa", informe para la Comisión Kofi Annan sobre Elecciones y Democracia en la Era Digital, 2019. **4** Bosch, Dendere y Mare, "The Effect of Social Media on Democracy and Elections in Africa". **5** Comisión Global sobre Elecciones, Democracia y Seguridad, "Profundizando la democracia: una estrategia para mejorar la integridad electoral en el mundo" (Ginebra: Fundación Kofi Annan, 2012). **6** *Electoral Integrity Assessments,* Fundación Internacional para Sistemas Electorales, www.ifes.org/issues/electoral-integrity-assessments. **7** Comisión Global sobre Elecciones, Democracia y Seguridad, "Profundizando la democracia", págs. 24 a 26. La seguridad mutua como condición previa para la democracia procede de Robert Dahl, *La poliarquía: participación y oposición* (New Haven: Yale University Press, 1971). **8** James S. Fishkin, *Democracia y deliberación: nuevas perspectivas para la reforma democrática* (New Haven: Yale University Press, 1991). **9** Christopher H. Achen y Larry M. Bartels, *Democracy for Realists: Why Elections Do Not Produce Responsive Government* (Princeton: Princeton University Press, 2016). **10** Murat Somer y Jennifer McCoy, "Déjà vu? Polarization and Endangered Democracies in the 21st Century", *American Behavioral Scientist*, 62, núm. 1 (2018): págs. 3 a 15. **11** Anna Lührmann *et al*., "State of the World 2018: Democracy Facing Global Challenges", *Democratization*, 26, núm. 6 (2019): págs. 895 a 915. **12** Nolan McCarty, Keith T. Poole y Howard Rosenthal, *Polarized America: the Dance of Ideology and Unequal Riches* (Cambridge: MIT Press, 2006); Jacob Jensen *et al*., "Political Polarization and the Dynamics of Political Language: Evidence from 130 Years of Partisan Speech", *Brookings Papers on Economic Activity*, 43, núm. 2 (2012): págs. 1 a 81; Matthew Gentzkow, "Polarization in 2016", libro blanco, *Toulouse Network for Information Technology*, 2016. **13** Yochai Benkler, Robert Faris y Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (Nueva York: Oxford University Press, 2018). **14** Benkler, Faris, y Roberts, *Network Propaganda*. **15** Benkler, Faris, y Roberts, *Network Propaganda*. **16** Edda Humprecht, "Where 'Fake News' Flourishes: A Comparison Across Four Western Democracies", *Information, Communication, and Society*, 22, núm. 13 (2019): págs. 1973 a 1988. **17** Humprecht, "Where 'Fake News' Flourishes", págs. 1973 a 1988. **18** Lührmann *et al*., "Democracy Facing Global Challenges", págs. 895 a 915. **19** Noam Gidron, James Adams, y Will Horne, "Toward a Comparative Research Agenda on Affective Polarization in Mass Publics", *APSA Comparative Politics Newsletter*, 29 (2019): págs. 30 a 36; Jennifer McCoy y Murat Somer, "Toward a Theory of Pernicious Polarization and How It Harms Democracies: Comparative Evidence and Possible Remedies", *The ANNALS of the American Academy of Political and Social Science*, 681, núm. 1 (2019): págs. 234 a 271. **20** Nic Newman *et al*., "Reuters Institute Digital News Report 2019", *Reuters Institute for the Study of Journalism*, 2019; Ronald Inglehart *et al*., *World Values Survey: All Rounds-Country-Pooled Datafile 1981-2014*, (Madrid: JD Systems Institute, 2014).

21 Pippa Norris, *Why Electoral Integrity Matters* (Cambridge: Cambridge University Press, 2014). **22** McCarty *et al*., *Polarized America*, págs. 78 a 81. **23** Herman Winkler, "The Effect of Income Inequality on Political Polarization: Evidence from European Regions, 2002-2014", *Economics and Politics*, 31, núm. 2 (2019): págs. 137 a 162. **24** Benjamin Reilly, *Democracy in Divided Societies: Electoral Engineering for Conflict Management* (Cambridge: Cambridge University Press, 2001); Lee Drutman, "The Case for Proportional Voting", *National Affairs*, 34 (2017): págs. 50 a 63. **25** Ryan D. Enos, *The Space between Us: Social Geography and Politics* (Cambridge: Cambridge University Press, 2017); Dante J. Scala y Kenneth M. Johnson, "Political Polarization along the Rural-Urban Continuum? The Geography of the Presidential Vote, 2000–2016", *The ANNALS of the American Academy of Political and Social Science*, 672, núm. 1 (2017): págs. 162 a 184. **26** Jonas Pontusson y David Rueda, "Inequality as a Source of Political Polarization: A Comparative Analysis of Twelve OECD Countries", *Democracy, Inequality, and Representation*, eds. Pablo Beramendi y Christopher J. Anderson (Nueva York: Russell Sage Foundation, 2008), págs. 312 a 353. **27** Drutman, "The Case for Proportional Voting". **28** McCoy y Somer, "Toward a Theory of Pernicious Polarization", págs. 234 a 271. **29** Cass R. Sunstein, *Republic.com* (Princeton: Princeton University Press, 2001). **30** Carole Cadwalladr, "Google Is Not 'Just' a Platform. It Frames, Shapes and Distorts How We See the World", *The Guardian*, 11 de diciembre de 2016, secc. "Opinion", https://www.theguardian.com/commentisfree/2016/dec/11/google-frames-shapes-and-distorts-how-we-see-world. **31** Kelly Weill, "How YouTube Built a Radicalization Machine for the Far-Right". *The Daily Beast*, 17 de diciembre de 2018, https://www.thedailybeast.com/how-youtube-pulled-these-men-down-a-vortex-of-far-right-hate. Véase también Kevin Roose, "The Making of a YouTube Radical", *The New York Times*, 8 de junio de 2019, https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html **32** Richard Fletcher y Rasmus Kleis Nielsen, "Are People Incidentally Exposed to News on Social Media? A Comparative Analysis", *New Media & Society*, 20, núm. 7 (2018): págs. 2450 a 2468. **33** Matthew Barnidge, "Exposure to Political Disagreement in Social Media versus Face-to-Face and Anonymous Online Settings", *Political Communications*, 34, núm. 2 (2017): págs. 302 a 321. **34** Pablo Barberá, "How Social Media Reduces Mass Political Polarization. Evidence from Germany, Spain, and the U.S.", documento de trabajo, 2014. **35** Christopher A. Bail *et al*., "Exposure to Opposing Views on Social Media can Increase Political Polarization", *Proceedings of the National Academy of Sciences*, 115, núm. 37 (2018): págs. 9216 a 9221. **36** Manoel Horta Ribeiro *et al*., "Auditing Radicalization Pathways on YouTube", 2019, http://arxiv.org/abs/1908.08313 **37** Kevin Munger y Joseph Phillips, "A Supply and Demand Framework for YouTube Politics", documento de trabajo, 2019. **38** "Public Statement from the Co-Chairs and European Advisory Committee of Social Science One", 11 de diciembre de 2019, https://socialscience.one/blog/public-statement-european-advisory-committee-social-science-one **39** Jenni Marsh y Tara Mulholland, "How the Christchurch Terrorist Attack Was Made for Social Media", *CNN*, 16 de marzo de 2019, https://www.cnn.com/2019/03/15/tech/christchurch-internet-radicalization-intl/index.html; Kevin Roose, "On Gab, an Extremist-Friendly Site, Pittsburgh Shooting Suspect Aired His Hatred in Full", *The New York Times*, 28 de octubre de 2018, https://www.nytimes.com/2018/10/28/us/gab-robert-bowers-pittsburgh-synagogue-shootings.html.

40 Timothy McLaughlin, "How WhatsApp Fuels Fake News and Violence in India", *Wired*, 12 de diciembre de 2018, https://www.wired.com/story/how-whatsapp-fuels-fake-news-and-violence-in-india/. **41** Amalini De Sayrah, "Facebook Helped Foment Anti-Muslim Violence in Sri Lanka. What Now?", *The Guardian*, 5 de mayo de 2018, https://www.theguardian.com/commentisfree/2018/may/05/facebook-anti-muslim-violence-sri-lanka. **42** Paul Mozur, "A Genocide Incited on Facebook, With Posts From Myanmar's Military", *The New York Times*, 18 de octubre de 2018, secc. "Technology", https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html. **43** "Amnistía revela alarmante impacto de los abusos contra las mujeres en Internet", *Amnistía Internacional*, 20 de noviembre de 2017, https://www.amnesty.org/es/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/. **44** Adriane Van Der Wilk, "Cyber Violence and Hate Speech Online against Women", Comisión de Derechos de la Mujer e Igualdad de Género del Parlamento Europeo, septiembre de 2018, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf **45** David Kaye, "UN Experts Urge States and Companies to Address Online Gender-Based Abuse but Warn against Censorship", *ACNUDH*, 8 de marzo de 2017, www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21317&LangID=E. **46** "Toxic Twitter - The Silencing Effect", *Amnistía Internacional*, marzo de 2018, www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-5/. **47** Lauren Etter, "Rodrigo Duterte Turned Facebook Into a Weapon, With a Little Help from Facebook", *Bloomberg News*, 7 de diciembre de 2017, https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook **48** Carly Nyst y Nick Monaco, "State-Sponsored Trolling: How Governments are Deploying Disinformation as Part of Broader Digital Harassment Campaigns", *Institute for the Future*, 2018, http://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf **49** Nina Jankowicz, "How Disinformation Became a New Threat to Women", *World Policy*, 20 de diciembre de 2017, https://worldpolicy.org/2017/12/20/how-disinformation-became-a-new-threat-to-women/ **50** Amnistía Internacional, "Toxic Twitter - The Silencing Effect". **51** La resolución más reciente de la Corte Suprema contra la regulación del discurso de odio se basó en una decisión unánime de junio de 2017 sobre el caso *Matal c. Tam*, 52 EE.UU. (2017). https://www.supremecourt.gov/opinions/16pdf/15-1293_1o13.pdf **52** Daphne Keller y Paddy Leerssen, "Facts and Where to Find Them: Empirical Research on Internet Platforms and Online Speech", *Social Media and Democracy: The State of the Field*, eds. Nathaniel Persily y Joshua Tucker (Nueva York: Cambridge University Press, próxima publicación). **53** Steve Stecklow, "Why Facebook Is Losing the War on Hate Speech in Myanmar", *Reuters*, 15 de agosto de 2018, https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/. **54** Tarelton Gillespie, *Custodians of the Internet: Platforms, Content Moderation and the Hidden Decisions That Shape Social Media* (New Haven: Yale University Press, 2018). **55** Código de Conducta de la UE, *Comisión Europea*, 4 de febrero de 2019, https://ec.europa.eu/info/policies/justice-%20and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/countering-illegal-hate-speech-online_es **56** Keller y Leerssen, "Facts and Where to Find Them". **57** "Germany starts enforcing hate speech law", *BBC News*, secc. "Technology", 1 de enero de 2018, https://www.bbc.com/news/technology-42510868. **58** Daphne Keller, "Internet Platforms: Observations on Speech, Danger, and Money", Hoover Working Group on National Security, Technology, and Law, Aegis Series, documento núm. 1807 (2018): pág. 2.

59 David Kaye, "Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression" (junio de 2017): 4. https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf **60** Samantha Bradshaw, Lisa-Maria Neudert y Philip Howard, *Government Responses to the Malicious Use of Social Media*, *Centro de Excelencia de Comunicaciones Estratégicas de la OTAN*, noviembre de 2018, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/01/Nato-Report.pdf **61** David Kaye y Fionnuala Ni Aolain, "Mandates of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; and the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism", 2019, https://freedex.org/wp-content/blogs.dir/2015/files/2019/04/OL-AUS-04.04.19-5.2019-2.pdf. **62** Jacob Mchangama y Joelle Fiss, "Germany's Online Crackdowns Inspire the World's Dictators", *Foreign Policy*, 6 de noviembre de 2019, https://foreignpolicy.com/2019/11/06/germany-online-crackdowns-inspired-the-worlds-dictators-russia-venezuela-india/. **63** Access Now, "Joint Letter on Internet Shutdown in Uganda", *CIPESA*, 24 de febrero de 2016, https://cipesa.org/2016/02/joint-letter-on-internet-shutdown-in-uganda/. **64** Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India", 7 de febrero de 2019, https://ssrn.com/abstract=3330413. **65** Louise Matsakis e Issie Lapowsky, "Don't Praise the Sri Lankan Government for Blocking Facebook", *Wired*, 23 de abril de 2019, https://www.wired.com/story/sri-lanka-bombings-social-media-shutdown/. **66** Daniel Arnaudo *et al*., "Political and Economic Implications of Authoritarian Control of the Internet", en Jonathan Butts y Sujeet Shenoi, *Critical Infrastructure Protection VII.* (Berlín, Heidelberg: Springer Berlin Heidelberg, 2013), págs. 3 a 19. **67** Abdi Latif Dahir, "Internet Shutdowns Are Costing African Governments More than We Though", *Quartz Africa,* 28 de septiembre de 2017, https://qz.com/africa/1089749/internet-shutdowns-are-increasingly-taking-a-toll-on-africas-economies/. **68** Access Now, "Joint Letter on Internet Shutdown in Uganda". **69** Roderick Fanou *et al*., *OONI - Open Observatory of Network Interference*, 30 de abril de 2019, https://ooni.org/. **70** Ribeiro *et al*., "Auditing Radicalization Pathways on YouTube". **71** Christopher Ross, "Reshma Saujani's Ambitious Plan for Technology", *The Wall Street Journal*, 6 de noviembre de 2014, https://www.wsj.com/articles/reshma-saujanis-ambitious-plan-for-technology-1415237831. **72** "Girls Who Code: Annual Report 2018", https://girlswhocode.com/2018report/. **73** Ross, "Reshma Saujani's Ambitious Plan for Technology". **74** Kimiko de Freytas-Tamura, "Kenyan Election Official Is Killed on Eve of Vote", *The New York Times*, 31 de julio de 2017, secc. "World", https://www.nytimes.com/2017/07/31/world/africa/chris-musando-kenya-election-official-dead.html. **75** Nanjira Sambuli, "The Importance of Monitoring Online Hate Speech", *Deutsche Welle*, 3 de octubre de 2016, https://www.dw.com/en/the-importance-of-monitoring-online-hate-speech/a-19104789. **76** Ibíd. **77** Susan Benesch, "Countering Dangerous Speech to Prevent Mass Violence during Kenya's 2013 Elections", Berkman Center for Internet and Society, 9 de febrero de 2014, https://www.ushmm.org/m/pdfs/20140212-benesch-kenya.pdf. **78** Kagonya Awori, "Umati Final Report", *iHub Research*, junio de 2013, https://preventviolentextremism.info/sites/default/files/Umati%20Final%20Report.pdf. **79** Ibíd. **80** Luciano Floridi, "Fake News and a 400-Year-Old Problem: We Need to Resolve the 'Post-Truth' Crisis", *The Guardian*, 29 de noviembre de 2016, www.theguardian.com/technology/2016/nov/29/fake-news-echo-chamber-ethics-infosphere-internet-digital. **81** Hunt Allcott y Matthew Gentzkow, "Social Media and Fake News in the 2016 Election", *Journal of Economic Perspectives*, 31, núm. 2 (2017): págs. 211 a 36. **82** Stephen Coleman, "The Digital Difference: Media Technology and the Theory of Communication Effects", *Journal of Communication*, 67, núm. 6 (2017): E7-E8.

83 Ralph Schroeder, "Does Google Shape What we Know?", *Prometheus*, 32, núm. 2 (2014): págs. 145 a 160. **84** Tarleton Gillespie, "The Relevance of Algorithms", en: Tarleton Gillespie, Pablo J. Boczkowski y Kirsten A. Foot, eds. *Media Technologies: Essays on Communication, Materiality, and Society* (Cambridge: MIT Press, 2014), págs. 167 a 194. **85** Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (Nueva York: Knopf, 2016); James Williams, *Stand Out of Our Light: Freedom and Resistance in the Attention Economy* (Cambridge: Cambridge University Press, 2018). **86** Benkler, Faris y Roberts, *Network Propaganda*; Marchal *et al*., "Junk News during the EU Parliamentary Elections", *Oxford Internet Institute*, Data Memo 2019.3. **87** Craig Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook", *BuzzFeed News*, 16 de noviembre de 2016, www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook. **88** Joshua Tucker *et al*., "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature" (William and Flora Hewlett Foundation, 2018). **89** Claire Wardle y Hossein Derakhshan, "Information Disorder: Toward and Interdisciplinary Framework for Research and Policy Making", informe del Consejo de Europa DGI(2017)09. *Consejo de Europa*. https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html **90** Gordon Pennycook y David Rand, "Assessing the Effect of 'Disputed' Warnings and Source Salience on Perceptions of Fake News Accuracy", documento de trabajo, 2017, 10.2139/ssrn.3035384. **91** Allcott y Gentzkow, "Social Media and Fake News in the 2016 Election" **92** Andrew Guess, Brendan Nyhan y Jason Reifler, "Selective Exposure to Misinformation: Evidence from the Consumption of Fake News During the 2016 US Presidential Campaign", *Consejo de Investigación Europeo 9* (2018). **93** Samantha Bradshaw *et al*., "Sourcing and Automation of Political News and Information over Social Media in the United States, 2016-2018", *Political Communication* (2019): págs. 1 a 21. **94** Lisa-Maria Neudert, Philip Howard y Bence Kollanyi, "Sourcing and Automation of Political News and Information During Three European Elections", *Social Media+ Society 5*, núm. 3 (2019): 2056305119863147. **95** Freja Hedman *et al*., "News and Political Information Consumption in Sweden: Mapping the 2018 Swedish General Election on Twitter", *Oxford Internet Institute*, Data Memo 2018.3. **96** Caio Machado *et al*., "News and Political Information Consumption in Brazil: Mapping the First Round of the 2018 Brazilian Presidential Election on Twitter", *Oxford Internet Institute*, Data Memo 2018.4. **97** Caio Machado, "WhatsApp's Influence in the Brazilian Election and How It Helped Jair Bolsonaro Win". *Consejo de Relaciones Exteriores*, 13 de noviembre de 2018, www.cfr.org/blog/whatsapps-influence-brazilian-election-and-how-it-helped-jair-bolsonaro-win. **98** Chico Mares y Clara Becker, "Só 4 das 50 imagens mais compartilhadas por 347 grupos de WhatsApp são verdadeiras", https://piaui.folha.uol.com.br/lupa/wp-content/uploads/2018/10/Relat%C3%B3rio-WhatsApp-1-turno-Lupa-2F-USP-2F-UFMG.pdf **99** Rafael Evangelista y Fernanda Bruno, "WhatsApp and Political Instability in Brazil: Targeted Messages and Political Radicalization", Data-Driven Elections: Workshop Papers, *Surveillance Studies Centre*, 2019. https://www.sscqueens.org/sites/sscqueens.org/files/evangelista_bruno-2019-04.pdf **100** Vidya Narayanan *et al*., "Polarization, Partisanship and Junk News Consumption over Social Media in the US", *Oxford Internet Institute*, Data Memo 2018.1. **101** Andrew Guess, Jonathan Nagler y Joshua Tucker, "Less than you Think: Prevalence and Predictors of Fake News Dissemination on Facebook", *Science Advances 5*, núm. 1 (2019): eaau4586. **102** Guess, Nagler y Tucker, "Less than You Think". **103** Jamie Hitchen *et al*., "WhatsApp and Nigeria's 2019 Elections: Mobilizing the People, Protecting the Vote". Abuja: Centro para

la Democracia y el Desarrollo, https://www.cddwestafrica.org/whatsapp-nigeria-2019-elections/ **104** Bradshaw, Neudert y Howard, Government Responses to the Malicious Use of Social Media. **105** Nathaniel Persily y Joshua Tucker, "Introduction", en *Social Media and Democracy: The State of the Field*, eds. Nathaniel Persily y Joshua Tucker (Nueva York: Cambridge University Press, próxima publicación). **106** Andrew Chadwick, The Hybrid Media System: Politics and Power (Oxford: Oxford University Press, 2013). **107** Persily y Tucker, *Social Media and Democracy*. **108** Sam Wineburg, *Why Learn History (When It's Already on Your Phone)* (Chicago: University of Chicago Press, 2018), págs. 139 a 159. **109** "New Challenges for Democracy: Elections in Times of Disinformation", *Instituto Nacional Electoral*, junio de 2019, págs. 4 y 5. **110** Ibíd., pág. 7. **111** Ibíd., pág. 7. **112** Ibíd., pág. 8. **113** Ibíd., pág. 9. **114** Ibíd., pág. 12. **115** Ibíd., págs. 9 a 11. **116** Ibíd., págs. 12 y 13. **117** Ibíd., págs. 14 y 15. **118** Ibíd., pág. 16. **119** Vasu Mohan, Maya Jacobs, Tana Azuaje, Kyle Lemargie y Carla Chianese, "The Race Against SARA and Hoaxes in Indonesian Elections", documento de trabajo, *Fundación Internacional para Sistemas Electorales*, 20 de agosto de 2019, pág. 3. **120** Vasu Mohan y Catherine Barnes, "Countering Hate Speech in Elections: Strategies for Electoral Management Bodies", libro blanco, *Fundación Internacional para Sistemas Electorales*, enero de 2018, ivi. https://www.ifes.org/sites/default/files/2017_ifes_countering_hate_speech_white_paper_final.pdf **121** Ibíd., págs. 20 a 34. **122** Mohan *et al*., "The Race Against SARA and Hoaxes in Indonesian Elections", 4. **123** Ibíd., 6. **124** Fanny Potkin y Agustinus Beo de Costa, "Fact-checkers vs. hoax peddlers: a fake news battle ahead of Indonesia's election", *Reuters*, 10 de agosto de 2019, https://www.reuters.com/article/us-indonesia-election-fakenews- insight/fact-checkers-vs-hoax-peddlers-a-fake-news-battle-ahead-of-indonesias-election-idUSKCN1RM2ZE **125** Mohan *et al*., "The Race Against SARA and Hoaxes in Indonesian Elections", págs. 6 y 7. **126** Ibíd., pág. 8. **127** "Update on Local Election Results in West Kalimantan And Papua", informe núm. 50, *Institute for Policy Analysis of Conflict*, agosto de 2018, pág. 6. http://file.understandingconflict.org/file/2018/08/IPAC_Report_50_Update.pdf **128** Erika Franklin Fowler *et al*., "Political Advertising Online and Offline", documento de trabajo, https://web.stanford.edu/~gjmartin/papers/Ads_Online_and_Offline_Working.pdf **129** Jessica Baldwin-Philippi, "The Myths of Data-Driven Campaigning", *Political Communications*, 34, núm. 4 (2017): págs. 627 a 633. **130** Jeff Chester y Kathryn Montgomery, "Follow the Tech: Emerging Digital Practices in the 2020 Election", Data-Driven Elections: Workshop Papers, *Surveillance Studies Centre*, 2019. https://www.sscqueens.org/sites/sscqueens.org/files/chester_montgomery-2019-04.pdf **131** Cathy O'Neil, *Armas de destrucción matemática: cómo el Big Data alimenta la desigualdad y amenaza la democracia*. (Madrid: Capitán Swing, 2017). **132** Robert S. Mueller, "Report on the Investigation into Russian Interference in the 2016 Presidential Election (Vol. I of II)" (Washington, D. C.: Departamento de Justicia de los Estados Unidos, 2019). **133** Philip N. Howard, Bharath Ganesh y Dimitra Liotsiu, "The IRA, Social Media and Political Polarization in the United States, 2012-2018", *Computational Propaganda Research Project*, Universidad de Oxford, 2019, https://assets.documentcloud.org/documents/5632779/IRA-Report-2018.pdf; Renee DiResta *et al*., "The Tactics & Tropes of the Internet Research Agency", *New Knowledge*, libro blanco, 2018. **134** Shannon McGregor, Bridget Barrett y Daniel Kreiss, "Barely Legal: Digital Politics and Foreign Propaganda", documento de trabajo, 2019. https://digitalpoliticalethics.weebly.com/uploads/5/0/9/9/50994643/mcgregorbarrettkreissapsa19_submit.pdf **135** Nick Clegg, "Facebook, Elections and Political Speech". *Facebook Newsroom*, 24 de septiembre de 2019, about.fb.com/news/2019/09/elections-and-political-speech/. **136** "Read the Letter Facebook Employees

Sent to Mark Zuckerberg About Political Ads", *The New York Times*, 28 de octubre de 2019, www.nytimes.com/2019/10/28/technology/facebook-mark-zuckerberg-letter.html. **137** "Nigeria National Elections: 2015 Nigeria Election Observation Report", *International Republican Institute*, 28 de marzo de 2015, pág. 5. http://www.iri.org/2015%20Nigeria%20Election%20Observation%20Report/1/assets/basic-html/index.html#III **138** "Abuja Accord On the Prevention of Violence and Acceptance of Elections Results by Presidential Candidates and Chairpersons of Political Parties contesting the 2015 General Elections", *Instituto Internacional para la Democracia y la Asistencia Electoral*, 2015, https://www.idea.int/sites/default/files/codesofconduct/Abuja%20Accord%20January%202015.pdf **139** International Republican Institute, "Nigeria National Elections", pág. 5. **140** Instituto para la Democracia y la Asistencia Electoral, "Abuja Accord", pág. 2. **141** International Republican Institute, "Nigeria National Elections", pág. 6. **142** The Associated Press, "Mozambique Peace Accord Is Signed, Paving Way for Elections", *The New York Times*, 6 de agosto de 2019, www.nytimes.com/2019/08/06/world/africa/mozambique-peace-accord-signed-paves-way-for-elections.html. **143** International Republican Institute, "Nigeria National Elections", pág. 5. **144** Fidelis Mbah, "Nigeria Elections: Presidential Candidates Sign 'Peace Deal'", *Al Jazeera*, 13 de febrero de 2019, www.aljazeera.com/news/2019/02/nigeria-elections-presidential-candidates-sign-peace-deal-190213154706618.html. **145** Michael McFaul y Bronte Kass, "Understanding Putin's Intentions and Actions in the 2016 US Presidential Election", en: Michael McFaul, *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond*, 2019, págs. 1 a 16. **146** "HPSCI Minority Open Hearing Exhibits", Comité Selecto Permanente de Inteligencia de la Cámara de Representantes de los Estados Unidos (HPSCI), informe minoritario, 1 de noviembre de 2017. **147** Shelby Grossman, Daniel Bush, y Renée DiResta, "Evidence of Russia-Linked Influence Operations in Africa", *Stanford Internet Observatory*, 29 de octubre de 2019. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf **148** Steven Lee Myers y Paul Mozur, "China Is Waging a Disinformation War Against Hong Kong Protesters", *The New York Times*, 14 de agosto de 2019, https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html **149** FireEye Intelligence, "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East", *FireEye Threat Research*, 21 de agosto de 2018, https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html **150** Adam Satariano, "Ireland's Abortion Referendum Becomes a Test for Facebook and Google", *The New York Times*, 25 de mayo de 2018, https://www.nytimes.com/2018/05/25/technology/ireland-abortion-vote-facebook-google.html **151** Hannes Grassegger y Mikael Krogerus, "The Data That Turned the World Upside Down", *Vice News*, 28 de enero de 2017, www.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win. **152** Colin Bennett y Smith Oduro-Marfo, "Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities", documento de la Oficina del Comisionado de Información del Reino Unido presentado en la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad de 2019 (ICDPPC), https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf **153** Baldwin-Philippi, "The Myths of Data-Driven Campaigning"; Daniel Kreiss, "Micro-Targeting, the Quantified Persuasion", *Internet Policy Review*, 6, núm. 4 (2017): págs. 1 a 14. **154** Tactical Tech Data and Politics Team, "Personal Data: Political Persuasion. Inside the Influence Industry", *Tactical Tech*, https://ourdataourselves.tacticaltech.org/posts/inside-the-influence-industry

155 Samantha Bradshaw y Philip Howard, "The Global Disinformation Disorder: 2019 Global Inventory of Social Media Manipulation", *Oxford Internet Institute Working Paper 2019.3*. Oxford, Reino Unido: Project on Computational Propaganda. **156** Jane Lytvynenko y Logan McDonald, "Hundreds Of Propaganda Accounts Targeting Iran And Qatar Have Been Removed From Facebook", *BuzzFeed News*, 7 de octubre de 2019, www.buzzfeednews.com/article/janelytvynenko/uae-propaganda. **157** Michael Riley, Lauren Etter y Bibhudatta Pradhan, "A Global Guide to State-Sponsored Trolling", *Bloomberg News*, 19 de julio de 2018, https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/ **158** Jonathan Corpus Ong y Jason Vincent A. Cabañes, "Architects of Networked Disinformation", *Newton Tech4Dev Network*, 2018, http://newtontechfordev.com/wp-content/uploads/2018/02/Architects-of-Networked-Disinformation-Executive-Summary-Final.pdf **159** Nic Cheeseman, Gabrielle Lynch y Justin Willis, "Digital Dilemmas: The Unintended Consequences of Election Technology", *Democratization*, 25, núm. 8 (2018): págs. 1397 a 1418. **160** Herbert Lin, Alex Stamos, Nathaniel Persily y Andrew Grotto, "Increasing the Security of the US Election Infrastructure", en: Michael McFaul, *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond*, 2019, págs. 17 a 26. **161** Ibíd. **162** Peter Wolf, "Cybersecurity and Elections: An International IDEA Round-Table", *Instituto para la Democracia y la Asistencia Electoral*, 8 de julio de 2017, www.idea.int/news-media/news/cybersecurity-and-elections-international-idea-round-table-summary. **163** Cheeseman, Lynch y Willis, "Digital Dilemmas", págs. 1397 a 1418.

En 2018, Kofi Annan, Presidente de la Fundación Kofi Annan, convocó la Comisión sobre Elecciones y Democracia en la Era Digital. La Comisión está compuesta por personalidades destacadas de los sectores público y privado, y de la sociedad civil, con experiencia de alto nivel en la esfera gubernamental, el sector tecnológico, el mundo académico y los medios de comunicación, a quienes el señor Annan encargó la realización de un estudio sobre las oportunidades y los desafíos que afronta la integridad electoral como resultado de los avances tecnológicos.

El presente informe recoge las principales conclusiones de la investigación y las consultas realizadas por la Comisión, junto con sus recomendaciones a fin de garantizar que las nuevas tecnologías, las plataformas de redes sociales y las herramientas de comunicación se puedan utilizar para materializar, y no inhibir, las aspiraciones de la ciudadanía de lograr una gobernanza democrática.

Publicado por

Kofi Annan FOUNDATION

Towards a fairer, more peaceful world