

Cómo pueden los miembros de la OGP hacer frente a la manipulación de información patrocinada desde el extranjero¹

Esta reseña de políticas forma parte de una serie de la Alianza para el Gobierno Abierto (Open Government Partnership, OGP) y el Instituto Nacional Demócrata para Asuntos Internacionales (National Democratic Institute, NDI) que analizan las medidas de apertura y supervisión que previenen o contrarrestan las influencias encubiertas extranjeras.

Resumen y descripción general

Los gobiernos autocráticos están planteando un desafío persistente y asimétrico a los gobiernos e instituciones democráticos en el ámbito de la información. La solidez de los sistemas de información abiertos de los que dependen las democracias está en juego. Las regulaciones y prácticas de apertura y supervisión pueden ayudar a contrarrestar el uso de la manipulación de información patrocinada desde el extranjero.

Índice

¿Qué es la manipulación de información patrocinada desde el extranjero?	1
¿Cuáles son los objetivos y las narrativas?	3
¿Cuáles son las tácticas?	4
¿Cómo la gobernanza democrática debilita la manipulación informativa patrocinada desde el extranjero?	7
Ejemplos de acciones para contrarrestar la manipulación de la información patrocinada desde el extranjero	8

¿Qué es la manipulación de información patrocinada desde el extranjero?

La manipulación de información patrocinada desde el extranjero implica el uso coordinado de medios de comunicación sociales o tradicionales para influir en el debate público mediante la difusión o amplificación intencionada de información falsa o engañosa; la participación en prácticas engañosas como ocultar o tergiversar el origen o la intención del contenido; o la elaboración y difusión de otras formas de contenido perjudicial, como el discurso de odio o la incitación a la violencia. También puede implicar la supresión intencional de información con fines políticos.

La manipulación de la información se ha convertido en una característica de la vida política en todo el mundo y un multiplicador de amenazas en otros ámbitos. La manipulación de la información suele ir de la mano de otros medios de influencia maligna, como el financiamiento encubierto o la corrupción política; los cuales se desarrollan a lo largo del tiempo, explotan las fracturas sociales y políticas, preparar a las audiencias para ataques futuros y se movilizan en momentos cruciales (como las elecciones). También requieren recursos significativos para su detección e investigación.



Ningún país ha escapado de los peligros de la manipulación de la información: ciudadanos de todo el mundo experimentan sus perjuicios a diario. La naturaleza opaca y las diversas tácticas dificultan la comparación entre países; sin embargo, un análisis de 2021 sobre la manipulación de la influencia realizada en Facebook entre 2017 y 2020 descubrió que los países que con mayor frecuencia fueron objeto de operaciones de influencia patrocinadas desde el extranjero fueron los Estados Unidos, el Reino Unido, Ucrania, Libia y Sudán.² Una encuesta global reciente muestra que casi el 60 % de los usuarios de Internet se preocupan por la información errónea.³ Como era de esperar, la ciudadanía de países con gobiernos democráticos son los que expresan mayor preocupación. Respetuosas de la libertad de información y expresión, y conscientes de las inquietudes relacionadas con la privacidad, las sociedades abiertas son más vulnerables a la manipulación de la información y menos propensas a responder controlando la información y las tecnologías.⁴

Si bien la manipulación nacional de la información es probablemente más común que los esfuerzos de influencia respaldados por el estado, la cantidad y el alcance de los gobiernos que llevan a cabo operaciones encubiertas en otros países no son insignificantes.⁵ En 2020, un grupo de investigadores identificó al menos siete países que utilizaban la manipulación de la información para influir en las opiniones fuera de sus fronteras.⁶

Es importante tener en cuenta que los actores estatales no son los únicos autores de la manipulación de la información extranjera. Los regímenes autoritarios a menudo dependen de empresas privadas especializadas en la venta de manipulación digital.⁷ Impulsados principalmente por las ganancias, estos actores privados pueden no tener los mismos objetivos que los actores estatales, pero sus campañas de manipulación de la información contribuyen a erosionar la confianza en las noticias y a debilitar el discurso democrático genuino. En varios contextos, las operaciones de información extranjeras también se han fusionado con las nacionales, por lo que una variedad de actores buscan tácticas similares, a menudo a través de la colaboración. Las empresas de redes sociales han identificado redes de manipulación de información encubierta afiliadas con partidos políticos, movimientos sociales y organizaciones religiosas.⁸



¿Cuáles son los objetivos y las narrativas?

Los gobiernos autoritarios manipulan la información para promover sus objetivos geopolíticos, cambiando la opinión global, sembrando discordias y conflictos y debilitando la confianza en la democracia.

Una narrativa común de estas operaciones es que los gobiernos democráticos son débiles e ineficaces. A fin de establecer una falsa equivalencia con sus regímenes no democráticos, los gobiernos autocráticos recurren al “whataboutism” (¿y qué pasa con?), la práctica de responder a una acusación con una contraacusación o planteando un problema diferente, para calificar de hipócritas a los gobiernos democráticos, en particular cuestiones de índole racial en el caso de los Estados Unidos.⁹ Durante la pandemia de COVID-19, cuando las vacunas se comenzaron a distribuir por todo el mundo, influencers’ simpatizantes de los gobiernos autoritarios trataron de socavar los registros de seguridad y eficacia de ciertas vacunas occidentales con el fin de aumentar el escepticismo sobre ellas y socavar su atractivo.¹⁰ En 2021, tanto Rusia como China fueron sofisticados en la adaptación de sus mensajes sobre las vacunas para dirigirse al público del sur global. Los medios de comunicación estatales chinos destacaron los desafíos del almacenamiento de la cadena de frío en países cálidos y cuestionaron los motivos de los fabricantes farmacéuticos en lugares con una historia de anticapitalismo.¹¹ Pekín también posicionó sus propias vacunas como bienes públicos globales de fácil acceso disponibles para los países en desarrollo en un momento en el que no estaba cumpliendo con su obligación de entrega. A lo largo de 2020, ambos países también destacaron las escenas de caos electoral en los Estados Unidos. El objetivo de estos esfuerzos es disminuir el atractivo de los sistemas democráticos, socavar sus instituciones y generar desconfianza en su modelo.



¿Cuáles son las tácticas?

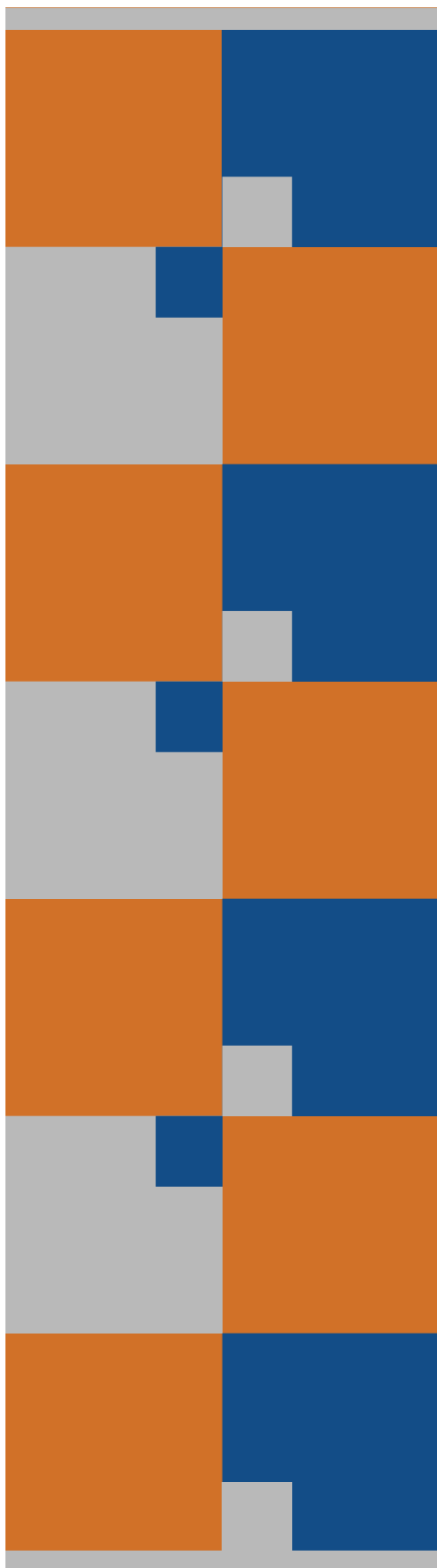
Los actores autoritarios realizan operaciones encubiertas de información a través de una amplia variedad de tácticas, a menudo implementando múltiples estrategias superpuestas contra un mismo objetivo.

Las formas más comunes de influencia incluyen los siguientes tipos de canales y actores:

Inversiones en vastos sistemas de propaganda. Los regímenes autoritarios han invertido inmensos recursos en sistemas mediáticos respaldados por el estado. En 2021, Moscú aumentó su presupuesto de propaganda a aproximadamente 2800 millones de USD, un aumento de 460 millones de USD con respecto a años anteriores.¹² Pekín, por su parte, ya en 2009 destinó hasta 6000 millones de USD a expandir los medios de comunicación estatales en todo el mundo.¹³ Tanto los medios de comunicación estatales rusos como los chinos han dominado los resultados de los motores de búsqueda para términos geopolíticamente destacados, dado que los motores de búsqueda están contruidos para priorizar el contenido “más fresco” o más reciente.¹⁴ Irán también ha surgido como un actor con ambiciones globales y una sofisticada propaganda digital, que apunta a al menos 15 países y que llega hasta América Latina.¹⁵

Agentes influyentes. Los gobiernos autoritarios utilizan una red de personas influyentes, en su mayoría occidentales, para impulsar el alcance y la resonancia de sus mensajes, agregando una apariencia de legitimidad y eliminando cierto grado de culpabilidad.¹⁶ Los actores autoritarios amplifican los sitios web, el contenido de las redes sociales, las cuentas y las redes marginales con el mismo fin. La Agencia Sueca de Investigación de Defensa ha identificado numerosos grupos de expertos rusos con vínculos establecidos con académicos y grupos marginales occidentales, que tratan de influir en círculos políticos de élite.¹⁷ Pekín ha creado discretamente una red de personalidades de redes sociales en Facebook, TikTok y Twitter, que reflejan la perspectiva del gobierno chino en publicaciones vistas por cientos de miles de personas.¹⁸ Estas personas influyentes trabajan para dar una imagen positiva de China, desviar las críticas de su historial de derechos y promover las opiniones de Pekín sobre una amplia gama de temas políticos.

Voces nacionales. Los actores autoritarios recurren a voces e instituciones nacionales auténticas para dar la impresión de que sus campañas de información son auténticas actividades de promoción, en parte para evadir las capacidades de detección de las plataformas y en parte para aumentar la percepción de legitimidad del contenido que promueven. Es posible que también deseen exacerbar la politización de los debates sobre moderación de contenido.¹⁹ Moscú, por ejemplo, lleva a cabo esta tarea ocultando trolls entre la población objetivo, alquilando las cuentas de redes sociales de ciudadanos locales o reclutando a verdaderos activistas para avivar las protestas.²⁰ Antes de las elecciones presidenciales de Madagascar en 2018, los agentes rusos reclutaron a un líder de una secta para que se postulara como candidata en un intento por dividir el voto de la oposición, pagaron a jóvenes locales para que asistieran a reuniones y contrataron a periodistas para que cubrieran esos eventos.²¹



Influencia local. Cada vez más, los esfuerzos rusos de manipulación de la información parecen dirigirse a personas influyentes dentro de una sociedad, por ejemplo, periodistas y activistas, en lugar de depender de grandes volúmenes de contenido de granjas trolls.²² Para ello, el Kremlin, por ejemplo, trabaja para llamar la atención de auténticas personas influyentes en varias plataformas de redes sociales. En Europa, los actores rusos se han hecho pasar por lugareños, y a veces por ciudadanos periodistas, para ponerse en contacto con periodistas y otros legisladores, por ejemplo, y utilizaron estas cuentas para crear y gestionar grupos y páginas, y para publicar y comentar contenido.²³ Luego, utilizaron diferentes activos para amplificar las publicaciones a audiencias específicas en varias plataformas.²⁴

Trolls. Arabia Saudita desarrolló una amplia red de trolls para promover la imagen del régimen y fomentar los objetivos estratégicos del gobierno a nivel nacional e internacional.²⁵ El régimen saudí creó miles de cuentas falsas cuando cortó los vínculos con Qatar en 2017, y las utilizó para representar el descontento popular dentro del país.²⁶ Las operaciones patrocinadas desde el extranjero también pueden incluir trolls ubicados dentro de la población objetivo. Tras el hundimiento de un barco surcoreano en 2010, agentes norcoreanos utilizaron los números de registro de residentes surcoreanos para crear cuentas falsas y publicar mensajes destinados a socavar la credibilidad de Seúl.²⁷

Teorías de conspiración. Las operaciones de información a menudo promueven teorías conspirativas para cuestionar las versiones oficiales de los eventos políticos o para promover la idea de que la verdad es inescrutable. Un ejemplo reciente es la narrativa falsa, promovida por el Kremlin, de que Ucrania está desarrollando capacidades de armas biológicas con el apoyo del Pentágono. Moscú promocionó esta narrativa, que se acuñó en varios podcasts populares en los Estados Unidos, porque sirve para justificar la invasión de Rusia a Ucrania.²⁸

Información malintencionada. Los regímenes autoritarios difunden contenido que es técnicamente verdadero, pero que se presenta de una manera muy engañosa para manipular la percepción pública de los problemas geopolíticos. Por ejemplo, en 2021, Rusia, China e Irán difundieron con regularidad noticias sensacionalistas sobre inquietudes de seguridad en torno a ciertas vacunas occidentales y minimizaron el contexto atenuante.²⁹ Estas tácticas pueden ser tan perjudiciales como la desinformación absoluta, pero mucho más difíciles de verificar o de responder.

Piratería de la percepción. La piratería de la percepción es un esfuerzo por crear la impresión de una operación exitosa, ya sea que haya ocurrido o no. Los operadores de la información parecen reconocer que no necesitan perpetuar la manipulación a gran escala para crear la impresión de que lo hicieron, especialmente para sembrar dudas sobre un resultado electoral. Moscú se esforzó por aprovechar la expectativa generalizada de que podría ocurrir una interferencia electoral para afirmar que así fue, incluso en ausencia de una operación exitosa.³⁰ Por ejemplo, antes de las elecciones de mitad de mandato de 2018 en los EE. UU., un sitio web que afirmaba formar parte de la infame Agencia de Investigación de Internet de Rusia intentó difundir



el miedo a la intromisión electoral afirmando la existencia de una vasta operación que no existía.

Desbordar con conversaciones críticas. Mientras que algunas manipulaciones respaldadas por el estado se centran en mermar el atractivo de los estados y las instituciones democráticas, otras intentan suavizar la imagen de sus propios regímenes autoritarios y amortiguar las críticas a su historial de derechos humanos. Tanto Arabia Saudita como China utilizan una variedad de tácticas para inundar de contenido positivo las conversaciones sobre su historial de derechos humanos.³¹ Estos incluyen campañas de hashtag y cuentas de redes sociales dedicadas para ahogar los reproches a sus políticas represivas.

Censura y represión. Los gobiernos autoritarios también llevan a cabo campañas agresivas de censura y represión en sus países y supervisan y trabajan para desestabilizar a los exiliados en el extranjero, con el fin de evitar las críticas de su historial en materia de derechos.³² Irán practica la censura y la intimidación estatal, incluida la creación de unidades de ciberpolicía represivas y el acoso a los usuarios, sobre todo mujeres, por comportarse de maneras que el régimen percibe como “no islámicas”.³³ El régimen bielorruso ha clausurado medios de comunicación independientes, ha encarcelado a periodistas, ha cerrado Internet, ha bloqueado plataformas externas y ha prohibido informar en directo sobre acontecimientos clave.³⁴



¿Cómo socava la gobernanza democrática la manipulación informativa patrocinada desde el extranjero?

La manipulación de la información por parte de actores extranjeros y autocráticos puede socavar la gobernanza democrática a través de múltiples vías.³⁵ En primer lugar, a menudo tiene como objetivo aumentar la polarización política, lo que dificulta que las sociedades democráticas se gobiernen a sí mismas.³⁶ La polarización y la parálisis que a menudo resulta de ella pueden hacer que la gobernanza democrática parezca ineficaz y poco atractiva en contraste con las alternativas autoritarias.

En segundo lugar, la manipulación de la información por parte de actores extranjeros y autocráticos a menudo tiene como objetivo aumentar el escepticismo sobre la existencia de una verdad objetiva. Esto atenta contra el núcleo mismo de una democracia funcional, que depende de la idea de que la verdad es conocida y los ciudadanos pueden discernirla para tomar decisiones de autogobierno. Los autoritarios no tienen esa necesidad de un espacio informativo saludable para sobrevivir, lo que les brinda un cierto grado de inmunidad: pueden contaminar el espacio informativo sin preocuparse demasiado por el bien común de la información global.³⁷

En tercer lugar, la manipulación de la información por parte de actores extranjeros y autocráticos con frecuencia busca reducir la confianza en las instituciones democráticas, incluidos los gobiernos democráticos, pero también en los medios de comunicación independientes, públicos y privados, las organizaciones multilaterales e incluso la web abierta.³⁸ Esto también puede poner de manifiesto las fisuras internas, debilitando a las sociedades democráticas desde adentro.

En cuarto lugar, los actores autoritarios pueden manipular la información en apoyo de un candidato o partido político preferido. Los esfuerzos por inclinar la balanza electoral influyen en el ejercicio de la autoridad pública de maneras que favorecen al gobierno perpetrador sobre el interés público. La manipulación informativa destinada a influir en las elecciones y los debates de políticas subvierte el derecho de un votante a “formar una opinión de manera independiente y libres de toda violencia, amenaza de violencia, presión o manipulación de cualquier tipo”.³⁹

Los líderes políticos de las sociedades abiertas, y especialmente los reformistas democráticos, suelen ser objeto de múltiples campañas de larga duración para denigrarlos o hacer que parezcan débiles e ineficaces. Las investigaciones indican que los líderes autoritarios atacan de manera desproporcionada a las mujeres políticas y activistas.⁴⁰




Ejemplos de acciones para contrarrestar la manipulación de la información patrocinada desde el extranjero

Los siguientes son ejemplos de los tipos de compromisos que los miembros de la OGP pueden asumir para contrarrestar la manipulación de la información. Aunque se desarrollaron teniendo en cuenta las amenazas de origen extranjero, muchas de las medidas también son relevantes para contrarrestar la manipulación de la información de origen nacional.

Facilitar el intercambio de conocimientos en todo el gobierno

Los gobiernos pueden desempeñar un papel fundamental en la creación de nuevos organismos o en el fortalecimiento de los existentes, así como en el apoyo a acciones intergubernamentales para comprender mejor la manipulación de la información extranjera dentro y fuera de sus fronteras.

- ◆ **Creación de un comité asesor de integridad de la información:** Los legisladores pueden asignar a una unidad específica la tarea de convocar a un comité asesor que pueda identificar y abordar las tendencias en el espacio de la información en todas las funciones gubernamentales. Estos organismos deben incluir a representantes de la sociedad civil y del sector privado y estar facultados para funcionar solo en calidad de asesores. Deben centrarse en la actividad de los estados extranjeros, no en la de los actores nacionales.
- ◆ **Creación de grupos de trabajo interinstitucionales o interministeriales:** El ejecutivo puede ayudar a los responsables de la toma de decisiones de todo el gobierno a desarrollar una comprensión matizada de las causas y consecuencias complejas de la manipulación de la información patrocinada desde el extranjero mediante la creación de grupos de trabajo. Mediante la vinculación de diferentes agencias o ministerios que normalmente trabajan de forma aislada, la oficina ejecutiva puede generar mejor una imagen coordinada de la amenaza, reconociendo que la manipulación de la información es solo una herramienta de interferencia extranjera que a menudo se utiliza junto con otras, particularmente las operaciones cibernéticas. Esto puede agregarse al mandato de un organismo ya existente, si corresponde, o puede ser parte de un organismo nuevo.
 - ▮ Para garantizar que los grupos de trabajo no cumplan con este mandato de manera aislada, sería útil que un país aumentara su participación en los procesos de múltiples partes interesadas y otros organismos internacionales que trabajan en cuestiones de libertad de expresión, privacidad y tecnología. Para obtener una lista de los organismos relevantes, consulte el punto "Procesos internacionales y de múltiples partes interesadas" en "Recomendaciones para actores no gubernamentales" a continuación.
- ◆ **Creación de una comisión parlamentaria de investigación ad hoc:** Los legisladores pueden crear un comité específico para comprender los complejos problemas legales, técnicos y políticos que plantean



las amenazas de manipulación de información extranjera, así como para crear conciencia pública y generar recomendaciones. En 2018-19, el Comité Digital, Cultura, Medios de Comunicación y Deporte del parlamento del Reino Unido realizó una investigación de 18 meses sobre la desinformación causada por las “fuerzas malignas” que abarcó los derechos de las personas sobre su privacidad, cómo sus elecciones políticas podrían verse afectadas e influenciadas por la información en línea y la interferencia en las elecciones políticas tanto en el Reino Unido como en todo el mundo.⁴¹

Regulación de las plataformas de redes sociales

Para aumentar la transparencia y la responsabilidad pública de las plataformas de redes sociales, los gobiernos pueden aprobar una legislación que defina el contenido dañino, establezca cuándo y cómo se debe eliminar dicho contenido e imponga multas a las empresas que no sigan las normas. A la hora de aplicar tales medidas, **es esencial que los gobiernos cumplan con los estándares internacionales de derechos humanos que estipulan que cualquier restricción al derecho de libre expresión debe estar prevista por la ley y ser estrictamente necesaria para el respeto de los derechos o la reputación de los demás; o para la protección de la seguridad nacional o del orden público, o la salud y la moral públicas.**⁴² Estas restricciones también no deben ser discriminatorias, deben tener un límite de tiempo y estar sujetas a supervisión por parte de organismos nacionales o internacionales.⁴³

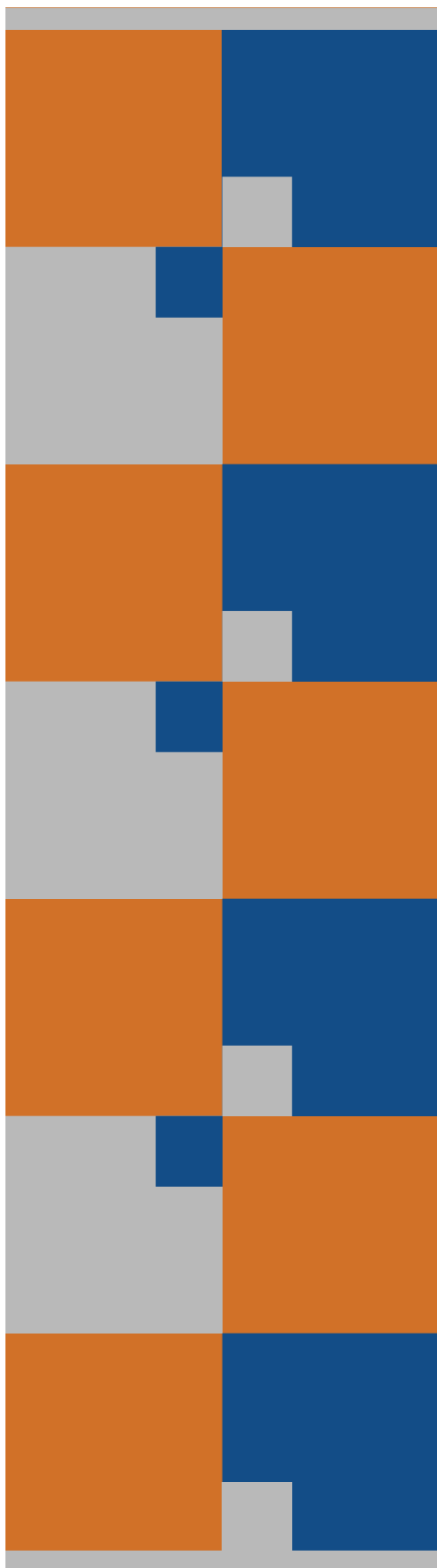
Protección de las libertades democráticas: Las medidas incluidas en este resumen representan un menú de opciones para los miembros de la OGP. Cualquier medida en consideración debe tener en cuenta la cultura política y las implicaciones para la libertad de expresión, la privacidad y otros derechos de los ciudadanos. Es particularmente importante garantizar que el recurso sea proporcional al problema y abstenerse de respuestas que puedan manipularse, por ejemplo, mediante la criminalización del discurso que amenaza al partido gobernante o a las fuerzas armadas. Las legislaturas nacionales deben garantizar que exista una vía legal para que las organizaciones de la sociedad civil (OSC) y las personas afectadas por las medidas puedan impugnar las leyes antipropaganda o cualquier medida que potencialmente restrinja la libertad de expresión.

Para disuadir o hacer frente a la retirada inadecuada de contenido o cuentas por parte del gobierno, las agencias reguladoras pueden crear, difundir y mantener estándares relacionados con la retirada de contenido o cuentas, y auditar el proceso mediante el cual los gobiernos solicitan dichas acciones. Los legisladores también pueden exigir la divulgación de solicitudes gubernamentales enviadas a redes sociales y medios de comunicación tradicionales para que tomen medidas para eliminar contenido o cuentas específicas. Los detalles sobre los informes de retirada en las redes sociales se pueden encontrar en la sección “Recomendaciones para actores no gubernamentales” a continuación.



◆ **Aprobación de la legislación para regular las plataformas de redes sociales:** Los legisladores pueden introducir políticas para contrarrestar la desinformación y el uso indebido (como las operaciones falsas, la manipulación política y la violencia en línea) de las plataformas de redes sociales. Existen numerosos ejemplos que pueden servir de lecciones para la legislación futura o sus enmiendas. Estos incluyen la Ley de Aplicación de la Red (NetzDG) de Alemania; el Reglamento General de Protección de Datos de la UE, el Paquete de la Ley de Mercados Digitales y Servicios Digitales; y la Ley de Intercambio de Material Violento Aborrecible de Australia.⁴⁴ A continuación se presentan ejemplos de algunas medidas de política:

- ▶ La legislación puede exigir a las empresas de redes sociales que informen regularmente sobre las decisiones de moderación de contenido con el fin de generar responsabilidad a través de la transparencia, mientras incentivan el comportamiento responsable por parte de las empresas. Los requisitos de presentación de informes pueden contribuir a desarrollar resiliencia a la manipulación de la información extranjera mejorando la comprensión colectiva de cómo funcionan las plataformas (y, por lo tanto, de las oportunidades de manipulación por parte de actores extranjeros), así como de las medidas de moderación de contenido que implementan para defenderse de la desinformación extranjera y otras campañas perjudiciales.
- ▶ La legislación también puede crear incentivos para que las empresas equilibren de manera responsable los intereses en las decisiones de moderación de contenido y equipen a los legisladores y al público para que exijan responsabilidades a las plataformas por no defenderse de manera responsable de la manipulación de información extranjera, incluso en contextos no occidentales.
- ▶ Los legisladores también pueden exigir que se informe sobre los anuncios, en particular la publicidad y algoritmos políticos, o los sistemas técnicos que moderan el contenido.
- ▶ Los legisladores subnacionales también pueden aprobar regulaciones impactantes, especialmente cuando representan provincias o estados importantes. Si bien en los Estados Unidos no existe una legislación federal o nacional de este tipo, la legislación a nivel estatal aprobada por California e Illinois también proporciona posibles modelos para abordar la manipulación de la información, incluidos los actores extranjeros.



Tenga cuidado con las leyes de imitación: Los gobiernos democráticos deben tener en cuenta que las regulaciones adoptadas en el país pueden utilizarse para justificar políticas que infringen los derechos digitales en otros lugares. Tomemos, por ejemplo, la NetzDG, una ley alemana que obliga a las plataformas de redes sociales con más de dos millones de usuarios a eliminar contenido “claramente ilegal” dentro de las 24 horas y todo el contenido ilegal dentro de los siete días de su publicación o se exponen a grandes multas. No solo creó incentivos para que las plataformas se inclinaran por retirar el contenido dudoso, sino que también provocó una proliferación de leyes de imitación en países considerablemente menos libres. Según un estudio, en solo unos meses, al menos 13 países adoptaron o propusieron modelos similares a NetzDG.⁴⁵ Ese año, Freedom House clasificó a cinco de esos países como “no libres” y cinco fueron clasificados como “parcialmente libres”. Este riesgo no debería evitar que los gobiernos democráticos promulguen normas, pero significa que deben ser prudentes en sus enfoques y planificar con anticipación para asegurarse de no dar inadvertidamente a los autócratas un tema de conversación o un plan para atacar el disenso o el pluralismo. Muchos casos examinados en la Guía para contrarrestar la desinformación del Consorcio para Elecciones y el Fortalecimiento de Procesos Políticos (Consortium for Elections and Political Process Strengthening, CEPPS) sobre enfoques legales y regulatorios muestran cómo se puede abusar de dichas leyes, pero también ofrecen posibles alternativas para regular la plataforma; por ejemplo, para proporcionar información electoral o para regular la publicidad y publicación de campaña.⁴⁶

- ◆ **Fortalecer los organismos y las funciones de supervisión existentes para controlar las tendencias de manipulación de la información y los abusos en la plataforma:** El fortalecimiento de la supervisión podría enfocarse en garantizar una mayor independencia de los organismos de supervisión audiovisual, así como en desarrollar los conocimientos necesarios para rastrear y exponer la manipulación de la información y hacer recomendaciones de políticas. En algunos países, estos pueden ser organismos gubernamentales (como las autoridades de protección de datos), organismos asesores de múltiples partes interesadas u organismos de supervisión convocados por el sector privado. En el Reino Unido, el mandato del regulador de las comunicaciones, Ofcom, se amplió para incluir también el monitoreo de los daños en línea. Algunos países carecen de organismos reguladores u organismos independientes con los conocimientos específicos necesarios para abordar la complejidad de la manipulación de la información nacional y extranjera. En estos casos, puede ser necesario crear una nueva agencia de supervisión experta para cubrir esta brecha. Como ejemplo a nivel estatal, California creó una Agencia de Protección de la Privacidad en 2020, mientras que



Australia creó un Comisionado de Seguridad Electrónica nacional en 2015. En muchos casos, estos organismos pueden remitirse a instancias judiciales y de derechos humanos que están en mejores condiciones de equilibrar la protección de la integridad de la información con otros derechos, como la libertad de expresión.

- ◆ **Fortalecimiento de la supervisión judicial o cuasi judicial de las violaciones de la plataforma:** Si una agencia experta no tiene la facultad de resolver disputas relacionadas con las violaciones en la plataforma, la legislación puede crear una vía para la aplicación judicial de la legislación relacionada con el contenido de las redes sociales en el contexto de otros derechos, incluida la libertad de expresión, la privacidad y la libertad de reunión. De acuerdo con los principios del gobierno abierto, estos tribunales deben permitir al público observar y registrar las quejas.

Estándares y orientación: legislación y estándares existentes sobre manipulación de la información

Para facilitar la auditoría externa de las prácticas de moderación de contenido y de los sistemas algorítmicos que recopilar información por parte de investigadores independientes, los legisladores podrían trabajar para impulsar medidas que mejoren la transparencia de la plataforma. Una reforma de transparencia que podría servir de modelo útil es la histórica Ley de Servicios Digitales (Digital Services Act, DSA) de la Unión Europea, que requeriría que las plataformas de redes sociales, entre otras cosas, divulguen cómo sus servicios amplifican el contenido divisivo.⁴⁷ También les exigiría que dejen de dirigir anuncios en línea basados en el origen étnico, la religión o la orientación sexual de una persona, lo que podría dar lugar a una mayor transparencia en la medida en que impida que los mensajes lleguen a audiencias limitadas sin el escrutinio por parte de un público más amplio. Además, exigiría a los llamados proveedores de servicios muy grandes que realicen auditorías anuales de los riesgos sistémicos que representan sus negocios.

En el futuro, los legisladores de todo el mundo podrían entablar un diálogo con sus contrapartes europeas sobre los enfoques para mejorar la transparencia de las plataformas con el fin de sacar lecciones de su experiencia reciente en el avance de marcos regulatorios. Reconociendo que esta ley tendrá un efecto global, los legisladores del sur global podrían considerar establecer medios de intercambio con los reguladores europeos

para garantizar que sus perspectivas estén representadas en el proceso.

Creación de ecosistemas mediáticos independientes y creíbles

Los legisladores pueden crear agencias independientes con independencia financiera del poder legislativo para supervisar los medios de comunicación subvencionados por el estado, como la televisión o la radio públicas. Esta y otras medidas para proteger la independencia de los medios públicos se describen con más detalle a continuación.

- ◆ **Prohibición de donaciones de propaganda extranjera:** los legisladores pueden aprobar leyes para crear y aplicar prohibiciones absolutas de “donaciones” de contenido de propaganda extranjera a redes de medios de comunicación estatales. Para obtener más detalles, consulte el recuadro siguiente sobre los enlaces entre las redes de propaganda prorrusa y una emisora de noticias pública en la República Eslovaca.
- ◆ **Medidas presupuestarias:** la introducción de la legislación a los presupuestos “reservados” (en este caso, donde los ingresos, costos y cuentas financieras de los medios de comunicación estatales están separados de la manipulación directa por parte del ejecutivo) puede limitar la capacidad de los funcionarios del gobierno de abusar de su acceso a los medios de comunicación estatales manipulando contenido a través de la coerción financiera.
- ◆ **Revisión periódica:** los legisladores también pueden establecer un sistema de revisión periódica de los canales de medios de comunicación estatales. Cuando no estén sujetas a revisión periódica, las normas deben limitar la interferencia con las operaciones cotidianas, la elaboración de presupuestos o la programación. Las normas también deben garantizar el cumplimiento de la veracidad de los informes y la transparencia de las donaciones y las fuentes de financiamiento. Algunos ejemplos de medios de comunicación estatales con revisión periódica son la British Broadcasting Corporation en el Reino Unido y la National Public Radio en los Estados Unidos.
- ◆ **Supervisión del defensor del pueblo/inspectorado público:** la creación de un defensor del pueblo específico dentro de las organizaciones de medios de comunicación puede proporcionar una función de supervisión crítica que es independiente de un organismo regulador, al recibir o investigar quejas relacionadas con la manipulación de la información. Los defensores del pueblo también pueden, si se les encarga, identificar problemas en todo el sistema del ecosistema de medios de comunicación independientes que pueden fomentar la propagación de la manipulación informativa nacional o extranjera en un país.
- ◆ **Pautas éticas y de calidad:** además de las normas y reglamentaciones formales, los medios de comunicación estatales a menudo establecen

estándares éticos y de calidad voluntarios para guiar su periodismo. Si bien en gran medida son inaplicables, estos valores pueden proporcionar un beneficio normativo a los medios estatales.

Revelación de la manipulación informativa prorrusa en los informativos públicos eslovacos

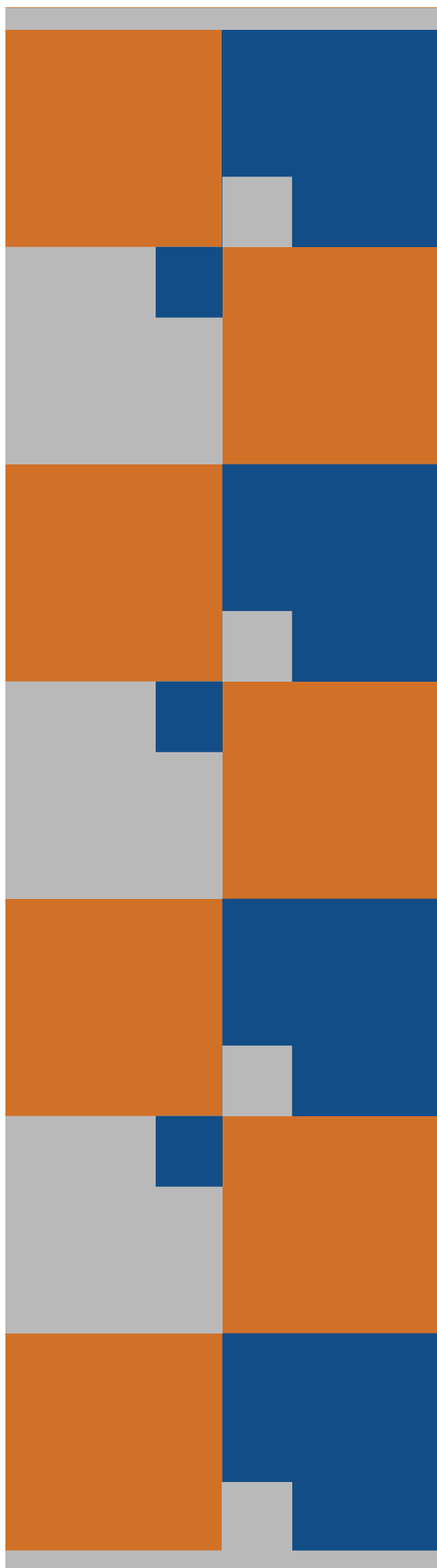
El caso de la República Eslovaca ilustra cómo la manipulación de la información extranjera puede socavar la credibilidad de un ecosistema de medios nacionales.⁴⁸ La agencia pública de noticias más grande del país, TASR, ha tenido conexiones preocupantes con medios de comunicación rusos.⁴⁹ Cabe destacar que se ha descubierto que TASR participa en la sutil promoción de la manipulación informativa rusa. Específicamente, TASR difunde informes de TASS, el servicio de noticias ruso, a menudo sin diferenciar el contenido de origen ruso del propio. Esto es particularmente problemático para las emisoras de medios locales que dependen de TASR para recibir noticias; sin esta diferenciación, las emisoras de noticias locales difunden inadvertidamente la manipulación informativa desde Rusia. Tras la invasión rusa de Ucrania, el gobierno eslovaco reforzó sus esfuerzos para combatir la desinformación. El gobierno creó el Centro para Combatir Amenazas Híbridas para analizar la desinformación y desarrollar estrategias para hacerle frente, entre otras medidas para crear recursos y marcos legales para detener su propagación.⁵⁰

Potenciar la participación de la sociedad civil

Los medios de comunicación y las organizaciones de la sociedad civil (OSC) pueden hacer un seguimiento de los patrones de manipulación de la información e identificar a los actores y redes malintencionados. Los medios de comunicación y las OSC también pueden exigir la responsabilidad pública de los gobiernos y las plataformas. Los legisladores pueden adoptar varias medidas para proteger y promover a los actores no estatales que luchan contra la manipulación de la información.

◆ Facilitar el diálogo público sobre problemas y soluciones

- ▶ **Audiencias sobre manipulación de la información y contramedidas:** los legisladores nacionales pueden crear oportunidades de diálogo que aprovechen el conocimiento de los medios de comunicación y las OSC convocando audiencias para comprender mejor el contexto específico en el que se propaga la manipulación de la información extranjera en un país determinado. Dichas audiencias también brindan la oportunidad de crear estrategias conjuntas para hacer frente a la manipulación de la información a través de la participación ciudadana.
- ▶ **Reuniones de recopilación de información:** los legisladores locales pueden organizar asambleas y otras reuniones de consulta pública con las OSC, los medios de comunicación



y otros representantes de interés público (o unirse a espacios de reuniones existentes que las OSC ya gestionan) para comprender la naturaleza y la escala de la manipulación de la información a un nivel más granular, que luego puede incorporarse a las políticas a nivel estatal o nacional.

◆ **Fortalecimiento de los derechos y las protecciones de los grupos que luchan contra la manipulación de la información**

- ◆ **Facilitar el compromiso de la sociedad civil con las plataformas:** los legisladores pueden reunir a un conjunto diverso de partes interesadas y capacitar a la sociedad civil; en particular, para contribuir al establecimiento de normas y compromisos. En 2018 y 2022, la Comisión Europea facilitó el diálogo entre la sociedad civil, las compañías de redes sociales y los grupos de investigación para desarrollar un Código de buenas prácticas en materia de desinformación.⁵¹
- ◆ **Obligación de divulgar los datos de beneficiarios finales de los medios de comunicación:** los legisladores pueden exigir la divulgación pública de los beneficiarios finales y los acuerdos de financiamiento de todos los medios de comunicación como un paso necesario para generar confianza y proteger contra la captura y la concentración del mercado. El acceso a los datos de beneficiarios finales permitirían que las OSC y los periodistas de investigación puedan identificar y responsabilizar a los actores negativos. Las políticas de beneficiarios finales y otros esfuerzos legislativos podrían servir de modelo para esta recomendación. Lo ideal sería que la transparencia de beneficiarios finales se extendiera a todas las empresas, en lugar de a las típicas grandes empresas a las que se dirige este tipo de supervisión basada en datos abiertos.
- ◆ **Protección de la libertad de expresión, los denunciantes y la reutilización de los datos:** los legisladores pueden aprobar o fortalecer las protecciones para ciudadanos, organizaciones, funcionarios públicos, actores del sector privado y medios de comunicación que enfrentan represalias. Las medidas específicas incluyen limitar las demandas por difamación e injurias; limitar los litigios estratégicos contra la participación pública (Strategic Litigation Against Public Participation, SLAPP); limitar las represalias contra los denunciantes y proporcionar incentivos para exponer el despilfarro, el fraude y el abuso; y llevar a cabo la supervisión para defender a los defensores de los derechos humanos.
- ◆ **Protección del derecho a la información:** la creación o el fortalecimiento de leyes de información oficial (también conocidas como “libertad de información” o “derecho a la información”) para garantizar el acceso público a la información gubernamental puede apoyar la rendición de cuentas para los gobiernos que participan en la manipulación de la información. Las excepciones a la información que pueda compartirse públicamente deben ser razonables.



◆ Presupuesto para capacitar a socios no estatales

- ◆ **Avance en la alfabetización digital:** en relación con el financiamiento para las OSC y los medios de comunicación, los legisladores pueden asignar fondos gubernamentales a programas de educación cívica y alfabetización digital que capaciten al público para identificar la desinformación y otras formas perjudiciales de contenido. Dada esa influencia, las campañas han cambiado de cuentas públicas a chats de grupos privados, proporcionar al público las herramientas para contrarrestar el contenido negativo, particularmente en sus propias redes, puede debilitar el efecto de la desinformación y sus contrapartes perjudiciales en el discurso público. Por su parte, las OSC pueden proporcionar información contrastada de hechos y otros recursos para aumentar el alcance de dichas iniciativas educativas, particularmente trabajando con grupos subrepresentados o en regiones a las que los gobiernos quizás no puedan llegar por sí solos.
- ◆ **Ofrecimiento de subvenciones a organizaciones que luchan contra la manipulación de la información:** los legisladores nacionales y locales pueden apoyar los esfuerzos de supervisión existentes proporcionando apoyo financiero a las OSC para llevar a cabo su trabajo, por ejemplo a través de subvenciones gubernamentales.

◆ Limitación de la legislación de represalias y contra la libertad de expresión:

los legisladores pueden promulgar leyes para limitar la capacidad del gobierno de abusar de las leyes de difamación e injurias, que pueden utilizarse para suprimir las críticas al gobierno bajo la apariencia de eliminar las “noticias falsas”. Los legisladores también pueden ofrecer una vía para que los ciudadanos interpongan recursos legales cuando los gobiernos aplican medidas de manipulación de la información para promover intereses perjudiciales. Los siguientes ejemplos ilustran cómo la falta de protecciones puede crear oportunidades para reprimir la disidencia.

- ◆ Como representante de una tendencia en todo el sudeste asiático, los legisladores de la Cámara de Representantes de Filipinas presentaron un proyecto de ley para penalizar la creación y difusión de “noticias falsas” a principios de agosto de este año.⁵² Organizaciones como Human Rights Watch expresado su preocupación por la falta de claridad en el proyecto de ley sobre cómo diferenciaría el gobierno entre contenido falso y verdadero.
- ◆ En 2019, el Parlamento de Tanzania modificó su Ley de Estadísticas de 2015, quizás en respuesta a la presión de las OSC locales e internacionales y las instituciones multilaterales.⁵³ La ley original y su enmienda en 2018 penalizaban la publicación de estadísticas sin la aprobación de la Oficina Nacional de Estadísticas.



Croacia: compromiso de las OGP sobre el marco de regulaciones de medios de comunicación (2018)

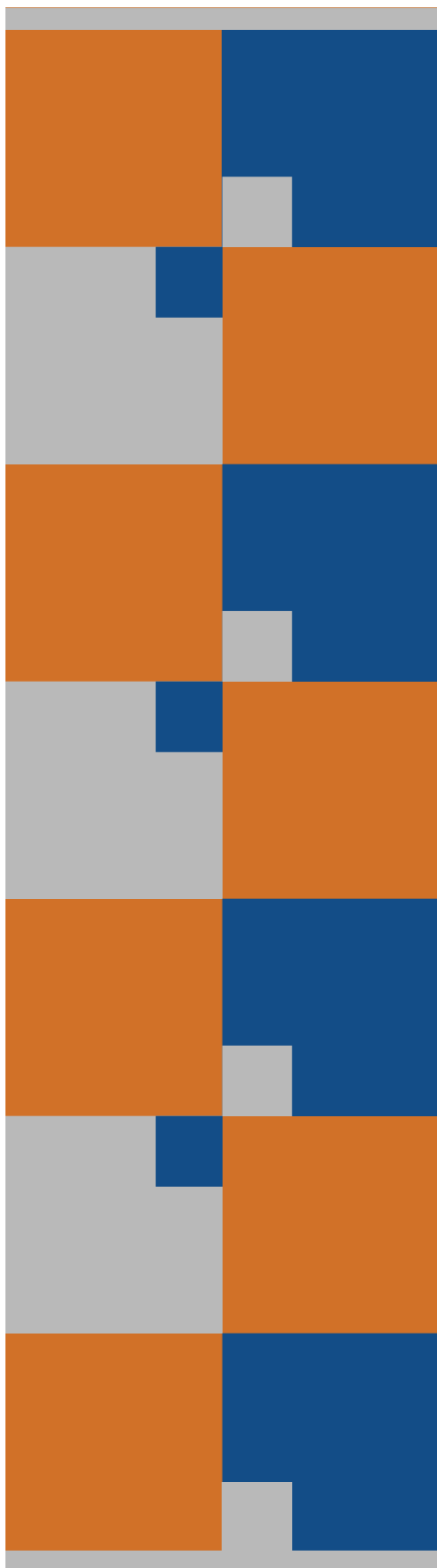
Las libertades de los medios de comunicación en Croacia han disminuido en los últimos años, debido, entre otras cosas, al aumento de la injerencia política en los medios ya las ataques contra periodistas.⁵⁴ El gobierno controla la mayoría de las fondos publicitarios a través de monopolios controlados públicamente, y las informes de prensa acusaron al gobierno de controlar secretamente la cobertura de las medias de comunicación de la respuesta del gobierno al brote de COVID-19.⁵⁵ También hay problemas relacionados con la ética y los estándares periodísticos, la falta de responsabilidad editorial y las crecientes problemas con las “noticias falsas”, particularmente en plataformas no lineales.

Croacia se comprometió a garantizar una mayor transparencia e independencia de la industria de las medias de comunicación en su tercer plan de acción de las OGP. Entre los hitos de este compromiso figuran la redacción de la legislación para aumentar la transparencia de las medias de comunicación y la creación de un registro de beneficiarios reales del sector. El compromiso también tiene como objetivo combatir las noticias falsas aumentando la confianza del público en las medias de comunicación y mejorando la alfabetización de los medios.

Ampliación de las protecciones de los datos y la supervisión del procesamiento de datos

Las autoridades de protección de datos (Data Protection Authorities, DPA) son organismos independientes que supervisan la aplicación de leyes de protección de datos. Aunque originalmente se concibieron para hacer frente a las violaciones de datos relacionadas con la seguridad estatal, el fraude (como la piratería de datos de las personas) y la privacidad, el mandato de las DPA se superpone con la desinformación a través de las formas en que los estados pueden abusar de los datos de los usuarios para la manipulación personalizada, incluso a través del “microtargeting” (microfocalización) de anuncios políticos, o mediante la piratería de información para utilizarla como arma en una operación de información.

- ◆ **Fortalecimiento de las DPA:** los legisladores deben considerar la creación de este tipo de organismos donde aún no existen o fortalecerlos para que puedan responder eficazmente a las violaciones de las leyes de protección de datos. Para ampliar la supervisión de las protecciones de datos y el procesamiento de datos (como la toma de decisiones automatizada), las DPA pueden proporcionar conocimiento experto de las cuestiones relacionadas con la protección de datos. Sin embargo, para asumir eficazmente este rol de supervisión, las DPA deben tener un mandato ampliado que vaya más allá de proporcionar asesoramiento experto, para evaluar si se han violado los principios de transparencia e imponer las sanciones que sean necesarias. A continuación, se presenta un resumen de estas posibles funciones.




- ▶ **Recepción de quejas y generación de informes:** esta función puede adoptar diferentes formas. Por ejemplo, las DPA pueden variar en términos de si los informes son periódicos, si pueden iniciarse a solicitud de otra agencia o si la DPA en sí puede iniciar un informe. Otra diferencia se relaciona con la recopilación de evidencia. El nivel de documentación que las DPA pueden obtener depende de si tienen poder de citación.
- ▶ **Empleo de herramientas de transparencia para algoritmos de redes sociales:** existen varias herramientas de transparencia emergentes que se utilizan para proteger los derechos humanos y prevenir los usos antidemocráticos de algoritmos.
 - ◆ **Registros de procesamiento de datos:** varios países exigen cada vez más registros de procesamiento algorítmico. Estos registros requieren que las agencias gubernamentales (y, en muchos casos, los actores del sector privado) divulguen qué datos se recopilan y cómo se procesan. En virtud de muchas leyes, el procesamiento de datos incluye la transferencia y reutilización de datos para publicidad política.
 - ◆ **Evaluación del impacto:** los actores del sector privado, los gobiernos y otros toman cada vez más medidas para garantizar que el procesamiento de datos mitigue los riesgos y los efectos negativos. Actualmente, en su mayoría se refieren a la privacidad y la piratería informática de datos confidenciales. Sin embargo, cada vez hay más interés en la transparencia en torno a las evaluaciones de impacto de los sesgos, los derechos humanos y la democracia. Los gobiernos pueden tomar iniciativas para exigir dichas medidas y avanzar hacia normas y estándares de evaluación, mitigación y consideración de alternativas. (Para un análisis más matizado de los enfoques y desafíos que plantea la evaluación de la toma de decisiones automatizada, consulte el trabajo realizado por AI Now Institute y Ada Lovelace Institute).⁵⁶ Algunos incluso han propuesto la introducción de una “evaluación del impacto de la democracia” de los algoritmos, tomando prestada la evaluación colectiva o ambiental de los daños ya adoptados en todo el mundo.⁵⁷
- ▶ **Ejecución de sanciones y recursos por violaciones:** según el alcance de su mandato, algunas DPA pueden llevar sus poderes de investigación de hechos un paso más allá para abordar la manipulación de información extranjera, especialmente cuando dicha manipulación puede constituir fraude o violar los estándares publicitarios. Las DPA pueden tener el mandato de derivar a un infractor de las leyes de protección de datos a una agencia de aplicación de la ley para su procesamiento, especialmente cuando se involucran sanciones civiles o penales. Las propias DPA con facultades de investigación, de procesamiento o de resolución judicial también pueden ordenar a una plataforma que retire el contenido manipulado a fin de proteger a la víctima. Es posible

que se necesite capacitación especializada del personal encargado de hacer cumplir la ley para garantizar respuestas adecuadas y protección de los derechos.

Mayor transparencia en elecciones y campañas

La manipulación de la información relacionada con las elecciones puede tener consecuencias de gran alcance, por lo que aquí se presta especial atención a esta forma de operación de la información. Aunque las recomendaciones que figuran a continuación se refieren principalmente a las responsabilidades de los organismos electorales (OE), garantizar la aplicación de estas medidas como complemento de las anteriores puede aumentar la eficacia de las contramedidas de un país.

- ◆ **Transparencia en el gasto de campaña política:** los OE pueden ampliar la transparencia de las campañas políticas y su financiamiento para abarcar nuevas tácticas de financiamiento, gasto y campaña tanto para los gastos de difusión digitales como los tradicionales. Una de esas tácticas de gasto es la contratación de firmas privadas de “comunicación estratégica”, a menudo en otros países, para impulsar narrativas de desinformación para favorecer una campaña.⁵⁸ Esta tendencia, de acuerdo con una encuesta de medios de comunicación de la Universidad de Oxford de 2020, es un problema global; la investigación descubrió que los actores estatales en el 56 % de los países encuestados (46 de 81) utilizaron estas firmas en campañas políticas.⁵⁹
- ◆ **Publicidad política en línea:** los legisladores deben elaborar reglamentos y pautas para la transparencia y la responsabilidad sobre el uso de la publicidad política en línea, que los OE puedan hacer cumplir. Los legisladores también deben establecer vías para que las agencias de supervisión, como los tribunales y las agencias reguladoras, identifiquen y regulen lo que constituye publicidad política aceptable.
- ◆ **Repositorios de anuncios políticos:** dado su poder para supervisar las elecciones de manera independiente, los OE pueden crear un repositorio universal de anuncios políticos. Dado que las campañas son multicanal y multiplataforma, un repositorio unificado permite una imagen completa y un debate crítico informado sobre el contenido y el financiamiento de anuncios políticos. Esta recomendación también puede facilitar los esfuerzos de supervisión dirigidos por otras organizaciones de medios de comunicación y las OSC, mejorando su acceso a la información sobre las campañas y sus prácticas publicitarias.
- ◆ **Exigencia de divulgación de las donaciones en especie de servicios de apoyo a las comunicaciones:** las políticas deben incluir cláusulas relacionadas con la divulgación de donaciones, incluidas cualquier “cosa de valor” en especie, particularmente de gobiernos extranjeros. Por ejemplo, los legisladores pueden obligar a declarar las donaciones monetarias y en especie (incluido el apoyo a las comunicaciones) y




aclarar jurídicamente qué se entiende por “cosas de valor”. También se debe divulgar cualquier acuerdo con gobiernos extranjeros.

- ◆ **Comunicación de resultados electorales veraces:** la oficina ejecutiva y sus administradores designados pueden aumentar la confianza en la integridad de la información que se origina en el gobierno a través de una comunicación transparente y proactiva. Esto es especialmente relevante en el contexto de las elecciones, que pueden estar respaldadas por medidas de supervisión de los OE.
 - Los ejemplos incluyen la creación de mesas de ayuda de información para que los periodistas verifiquen la información relacionada con las elecciones, o los recuentos rápidos de colaboración colectiva relacionados con las encuestas para garantizar que los resultados de las elecciones no se representen como un fraude (sobre todo por parte de un candidato perdedor).
- ◆ **Códigos de conducta de las campañas:** los OE pueden colaborar con las campañas para elaborar y promulgar códigos de conducta para las campañas en línea, que van desde el uso responsable de los macrodatos hasta el tratamiento de “deepfakes” (falsificación profunda) y filtraciones de información. Aunque son voluntarios, estos compromisos no solo pueden proporcionar apoyo adicional a un código electoral existente, sino que también incentivan a los candidatos y partidos políticos para que actúen de manera ética en sus campañas en casos en los que existan pautas o brechas inconsistentes en la ley.

Lucha contra la violencia en línea contra las mujeres (VCM)⁶⁰

La Violencia en Línea contra las Mujeres (VCM), ya sea de origen extranjero o nacional, plantea un desafío cada vez mayor para la democracia, sirviendo como una herramienta clave de agendas anti-derechos en todo el mundo. Esta forma de agresión en línea a menudo está dirigida específicamente contra las mujeres en la política, buscando excluirlas de la vida pública por el mero hecho de ser mujeres. Las plataformas tecnológicas son las que “más tienen que hacer” a la hora de implementar intervenciones para proteger a las mujeres que participan en política a través de sus plataformas, aunque los gobiernos también deben trabajar para comprender, crear conciencia y tomar las medidas adecuadas. Entre las posibles medidas de transparencia y supervisión se incluyen las siguientes:

- ◆ Las empresas de redes sociales deben medir e informar sobre la prevalencia del abuso de género; colaborar con organizaciones de verificación de hechos; proporcionar a los socios de investigación acceso permanente a los datos; y realizar y compartir evaluaciones de impacto sobre los derechos humanos enfocadas en el género en sus plataformas.
- ◆ Los gobiernos pueden incluir mecanismos específicos de



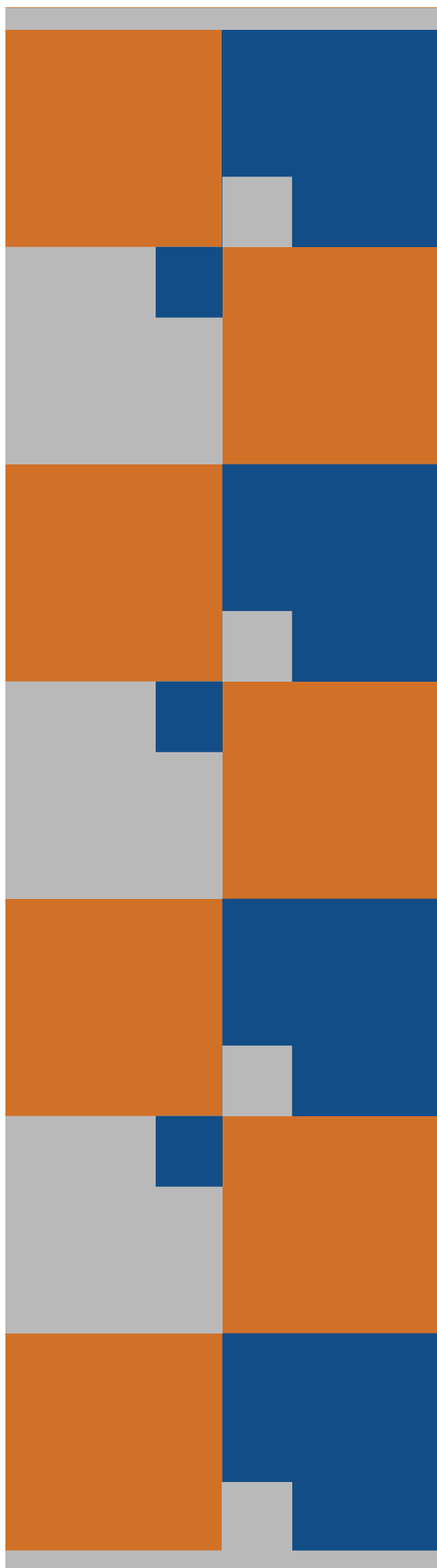
presentación de informes sobre la desinformación sexista en la legislación que aborda la transparencia de las plataformas de redes sociales.

Recomendaciones para actores no gubernamentales

Aunque este documento se centra principalmente en las medidas que pueden tomar los gobiernos para diagnosticar, tratar y prevenir la propagación de la manipulación de información extranjera, las siguientes recomendaciones abordan algunas medidas críticas que las partes interesadas no gubernamentales pueden tomar para reforzar estos esfuerzos.

Procesos internacionales y de múltiples partes interesadas: los procesos internacionales y de múltiples partes interesadas pueden ser herramientas útiles para respaldar las estrategias de lucha contra la desinformación. A continuación se presentan varias de estas iniciativas. Los miembros de las OGP pueden elegir sumarse a estas iniciativas multilaterales o reforzar su participación en ellas.

- ◆ **Principios de Santa Clara:** desarrollados por organizaciones de derechos humanos, defensores y expertos académicos, los Principios de Santa Clara apoyan los esfuerzos de las empresas por cumplir con los estándares de derechos humanos. Sus principios fundamentales incluyen varios relacionados con la transparencia, con ejemplos a continuación.⁶¹
 - ▶ En una ubicación de fácil acceso en sus sitios web, las empresas deben publicar normas y políticas claras relacionadas con cuándo moderarán el contenido.
 - ▶ Los usuarios deben saber cuándo un actor estatal ha solicitado o participado en alguna acción tomada sobre su contenido o cuenta.
 - ▶ Los usuarios deben saber cuándo los algoritmos han tomado decisiones de moderación de contenido en su totalidad o en parte. También deben comprender la lógica de la toma de decisiones de los procesos automatizados relacionados con la moderación del contenido.
- ◆ **Código de buenas prácticas de la UE en materia de desinformación:** Hasta la fecha han firmado más de 30 signatarios de distintos sectores (incluidas plataformas de redes sociales, miembros de la industria publicitaria y grupos de la sociedad civil).⁶² El código incluye compromisos para desmonetizar la desinformación; apoyar iniciativas de alfabetización informativa y mediática; y mejorar la divulgación de datos para la investigación sobre la desinformación, entre otras medidas. El código también establece un Centro de Transparencia accesible para todos los ciudadanos de la UE, para documentar el progreso hacia la implementación de las medidas del código.



- ◆ **Principios de la Iniciativa de Red Global (GNI):** GNI se lanzó en 2008 como un proceso de múltiples partes interesadas para desarrollar principios que las empresas de tecnología puedan seguir para garantizar que su toma de decisiones respete la libertad de expresión y los derechos de privacidad.⁶³ Los participantes de GNI son empresas de tecnología, las OSC (como organizaciones de libertad de prensa), académicos e inversionistas. Para obtener detalles, consulte las Pautas de implementación.⁶⁴
- ◆ **Principios de inteligencia artificial de la Organización para la Cooperación y el Desarrollo Económicos (OCDE):** los gobiernos de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), junto con otros miembros, se han comprometido a promover el desarrollo de IA confiable e innovadora que respete los derechos humanos y los valores democráticos.⁶⁵ Los principios también proporcionan recomendaciones para los legisladores, como orientación para invertir en investigación y desarrollo de IA.

Plataformas de redes sociales: las plataformas de redes sociales pueden complementar los procesos regulatorios utilizando las siguientes medidas:

- ◆ **Supervisión y publicación de datos de progreso:** las plataformas de redes sociales pueden utilizar un sistema de “medición, notificación y verificación” (Measurement, Reporting and Verification, MRV) para crear indicadores que se puedan medir metódicamente, notificar públicamente a los reguladores, los investigadores y al público, y verificarse a través de una revisión independiente. Por ejemplo, estos indicadores pueden realizar un seguimiento de las acciones de la plataforma relacionadas con la moderación de contenido, como la “Tasa de visualización de contenidos infractores” de YouTube, que busca determinar qué porcentaje de vistas en la plataforma provienen del contenido que viola sus políticas, para evaluar si los cambios en su algoritmo de moderación de contenido están impidiendo eficazmente que se vean videos perjudiciales.⁶⁶ Idealmente, estos indicadores se diseñarán con agencias reguladoras relevantes, grupos de expertos no gubernamentales y otras partes interesadas clave. El acceso a esta información permitiría a los investigadores independientes comprender mejor la naturaleza de diversos daños en línea y contribuiría en gran medida a aumentar la resiliencia de las sociedades democráticas. El acceso sólido de los investigadores a los datos también puede ayudar a los grupos académicos y de la sociedad civil a exponer campañas de información individuales, impidiendo que continúen y enseñando a los defensores cómo evolucionar y mejorar.
- ◆ **Transparencia en la retirada y la apelación:** dado que, en aras de la transparencia, los gobiernos deben facilitar datos de retirada sobre sus solicitudes, las plataformas de redes sociales también deben informar sobre la cantidad de solicitudes recibidas, la cantidad de cuentas o contenidos afectados por las solicitudes y cómo respondió la plataforma. Sería útil divulgar información relacionada con el alcance de las campañas de manipulación de la información (incluso



por parte de actores y redes extranjeras); aunque Facebook divulgó la cantidad de cuentas eliminadas y sus seguidores en su informe de amenazas de 2021, no describió la cantidad de vistas que recibieron las publicaciones de manipulación de la información.⁶⁷

- ▶ **Desglose de solicitudes gubernamentales:** separar las solicitudes gubernamentales de las solicitudes del sector privado (como aquellas relacionadas con reclamaciones de derechos de autor), que actualmente no es la norma. Para ver un ejemplo, consulte este informe de Google.⁶⁸
- ▶ **Creación (o fortalecimiento) de un proceso de apelación:** establecer procesos de apelación claros para garantizar que las solicitudes de retirada sean razonables y se ajusten a la ley y la política de la empresa. Para ver un ejemplo de cómo puede ser un proceso justo, transparente y accesible, consulte esta carta abierta a Mark Zuckerberg, redactada por los defensores de los Principios de Santa Clara.⁶⁹
- ◆ **Políticas de protección de los denunciantes:** las plataformas de redes sociales pueden adoptar estándares y pautas para proteger a las empresas que denuncien violaciones de la ley. La creación de canales internos para el disenso constructivo, especialmente en torno a cuestiones de desinformación y violaciones de los derechos humanos, es fundamental para garantizar la responsabilidad pública y la transparencia en la toma de decisiones de las empresas.
- ◆ **Apoyo a la investigación independiente:** las empresas de redes sociales pueden apoyar la investigación en múltiples contextos e idiomas. El estudio de la manipulación de la información se ha centrado en gran medida en los Estados Unidos y Europa, a pesar de que la mayoría de los usuarios de plataformas de redes sociales residen en otros lugares.⁷⁰ Es posible que los hallazgos de esa investigación no sean generalizables a otras democracias. Los investigadores podrían ser examinados por un tercero para confirmar su proyecto, experiencia y antecedentes, y posiblemente firmar acuerdos para garantizar que cuidarán los datos y seguirán las mejores prácticas éticas en su uso.



Cómo el gobierno taiwanés apoya los esfuerzos de verificación de hechos de las OSC

Un ejemplo de una asociación público-privada eficaz que aprovecha la experiencia de las OSC es el proyecto de Responsabilidad Digital, una colaboración entre el Yuan legislativo de Taiwán y organizaciones externas de verificación de hechos.⁷¹ El proyecto proporciona un servicio de verificación de hechos en la aplicación de mensajería de línea llamada “Verificador de hechos de línea”, que permite a los usuarios de línea cargar enlaces o estados de cuenta que pueden compararse automáticamente con contenido que ya ha sido verificado o escalado a revisión manual si fuera necesario.

Organizaciones de la sociedad civil: las OSC pueden contrarrestar la manipulación de información patrocinada desde el extranjero de diversas maneras:

- ♦ **Identificando narrativas y comportamiento no auténtico coordinado:** la sociedad civil, a menudo en colaboración con académicos u organizaciones de investigación, puede ayudar a desenmascarar las operaciones de información.⁷² Los OSC pueden realizar una supervisión de los medios para identificar narrativas clave y detectar comportamientos no auténticos coordinados. Dado que las mujeres y otros grupos subrepresentados suelen ser los primeros objetivos de las operaciones de información, las organizaciones cívicas que representan estos intereses están bien posicionadas para identificar la aparición de estas tácticas.⁷³
- ♦ **Llevando a cabo campañas de concientización pública/educación mediática:** la conexión de las OSC con las comunidades locales las posiciona para diseñar e implementar programas de concientización pública y educación mediática.⁷⁴ La mejora de la educación mediática y digital de las audiencias podría ayudar a reducir las susceptibilidades a la manipulación de la información con el tiempo.
- ♦ **Abogando ante el gobierno:** la defensa de la sociedad civil puede respaldar las políticas de transparencia y supervisión que sirven para contrarrestar las operaciones de información. Además, las OSC tienen un derecho crucial que desempeñar como guardianes y defensores para garantizar que las respuestas gubernamentales a las operaciones de información no representen infracciones no democráticas a la libre expresión o al acceso a la información.
- ♦ **Abogando ante empresas de redes sociales:** en función de su análisis de los patrones y los daños de la manipulación de la información, las OSC pueden abogar por cambios en la política de la plataforma que respondan a esos problemas específicos. Los enfoques de defensa basados en redes y coaliciones, particularmente a nivel internacional, pueden ayudar a aumentar la influencia a través de la acción colectiva.



Medios tradicionales: a través de sus informes de investigación, los medios de comunicación pueden desempeñar un papel importante en el desenmascaramiento y la concientización sobre la manipulación de la información. Los medios también deben evitar amplificar la manipulación de la información a través de sus informes. La manipulación de la información puede convertirse en su propio “ritmo”, lo que requiere conocimiento especializado y acceso a expertos para garantizar informes precisos. Al demostrar públicamente su transparencia y profesionalismo, los medios de comunicación también pueden ayudar al público a distinguir entre el periodismo legítimo y la manipulación de la información. La verificación de hechos, la atribución, la validación y la contextualización son requisitos del periodismo ético y fundamentales para generar confianza en el público. Los consejos de prensa o las organizaciones autorreguladoras de medios de comunicación tienen una responsabilidad importante de proteger la integridad y la calidad de los medios.

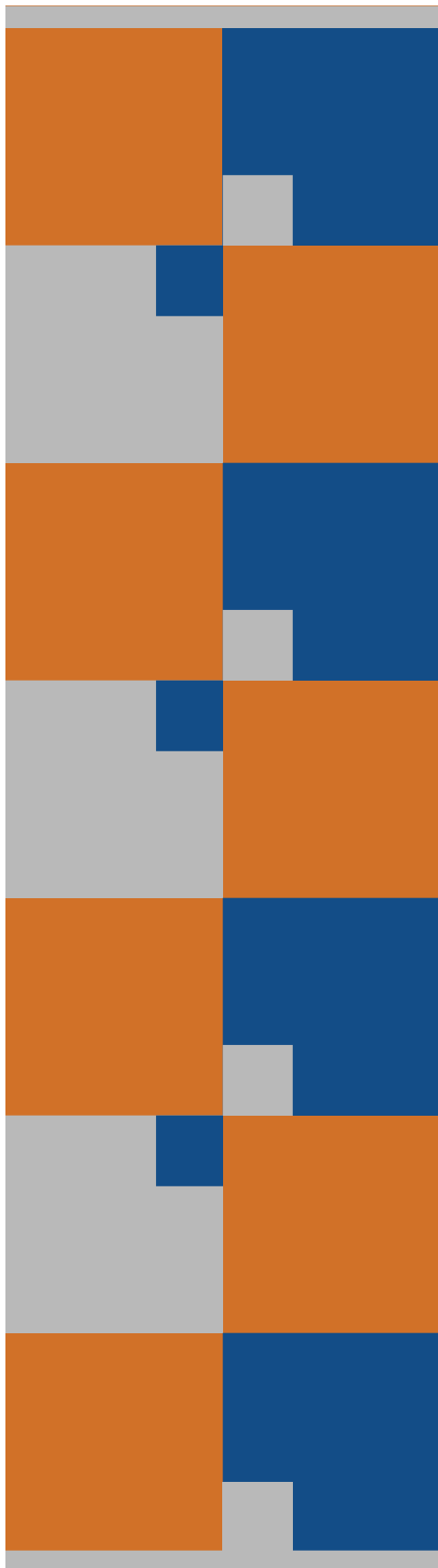
Filántropos y otros financiadores del sector privado: los actores filantrópicos y otras empresas del sector privado pueden apoyar la labor de los medios de comunicación libres e independientes, así como de los investigadores de la sociedad civil, para que continúen su trabajo. Dados los desafíos que afrontan muchas organizaciones de medios de comunicación y OSC para obtener una financiación estable, la filantropía o el sector privado podrían proporcionar apoyo financiero fundamental a través de subvenciones.

Notas finales

- 1 Los colaboradores incluyen a Jessica Brandt, Joseph Foti, Christina Socci, Corina Rebegea y Daniel Arnaudo.
- 2 “Threat Report: Combatting Influence Operations” (Informe de amenazas: lucha contra las operaciones de influencia), Meta, 26 de mayo de 2021, <https://about.fb.com/news/2021/05/influence-operations-threat-report/>.
- 3 Aleksu Knuutila, Lisa-Maria Nedert y Philip N. Howard, “Who Is Afraid of Fake News? Modeling Risk Perceptions of Misinformation in 142 Countries” (¿Quién le teme a las noticias falsas? Cómo modelar las percepciones de riesgo de la información errónea en 142 países), *Harvard Kennedy School Misinformation Review*, 12 de abril de 2022, <https://misinforeview.hks.harvard.edu/article/who-is-afraid-of-fake-news-modeling-risk-perceptions-of-misinformation-in-142-countries/>.
- 4 Jessica Brandt et al., “Linking Values and Strategy: How Democracies Can Offset Autocratic Advances” (Vincular valores y estrategia: cómo pueden las democracias contrarrestar los avances autocráticos (Alianza para asegurar la democracia, octubre de 2020), <https://securingdemocracy.gmfus.org/wp-content/uploads/2020/10/Linking-Values-and-Strategy.pdf>.
- 5 “Domestic Disinformation on the Rise in Africa” (Aumenta la desinformación nacional en África), Centro de Estudios Estratégicos de África, 6 de octubre de 2021, <https://africacenter.org/spotlight/domestic-disinformation-on-the-rise-in-africa/>.
- 6 Davey Alba y Adam Satariano, “At Least 70 Countries Have Had Disinformation Campaigns, Study Finds” (Al menos 70 países han tenido campañas de desinformación, según un estudio), *The New York Times*, 26 de septiembre de 2019, <https://www.nytimes.com/2019/09/26/technology/government-disinformation-cyber-troops.html>.
- 7 Hannah Bailey, Samantha Bradshaw y Philip N. Howard, “Industrialized Disinformation, 2020 Global Inventory of Organized Social Media Manipulation” (Desinformación industrializada, Inventario mundial 2020 de la manipulación organizada de las redes sociales), Proyecto de Investigación sobre Propaganda Computacional, Universidad de Oxford, 2020, <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/02/CyberTroop-Report20-Draft9.pdf>.
- 8 Josh Goldstein y Shelby Grossman, “How Disinformation Evolved in 2020” (Cómo evolucionó la desinformación en 2020), Institución Brookings, 4 de enero de 2021, <https://www.brookings.edu/techstream/how-disinformation-evolved-in-2020/>.
- 9 *Dictionary.com*, s.v. “whataboutism (n)” s.f., <https://www.dictionary.com/browse/whataboutism>.
- 10 Bret Schafer et al., “Influence-enza: How Russia, China, and Iran Have Shaped and Manipulated Coronavirus Vaccine Narratives” (Influencia-enza: cómo Rusia, China e Irán modelaron y manipularon las narrativas sobre la vacuna contra el coronavirus), Alianza para asegurar la democracia, 6 de marzo de 2021, <https://securingdemocracy.gmfus.org/russia-china-iran-covid-vaccine-disinformation/>.
- 11 Lin Jing (@CHINA_DIPLOMAT), “Cold truth: South Africa won’t be able to store Pfizer’s COVID vaccine. Here’s why” (Fría verdad: Sudáfrica no podrá almacenar la vacuna contra la COVID de Pfizer. He aquí el porqué), Twitter, 13 de noviembre de 2020, 4:34 a. m., https://twitter.com/CHINA_DIPLOMAT/status/1327183042444734465; Shen Shiwei (@shen_shiwei), “#Senetal is in talks to buy at least 200,000 doses of #COVID19 #vaccine developed by #China’s #Sinopharm” (#Senetal está en conversaciones para comprar al menos 200 000 dosis de #vacuna contra la #COVID19 desarrollada por #Sinopharm de #China), Twitter, 16 de enero de 2021, 12:37 a. m., https://twitter.com/shen_shiwei/status/1350316280977502208; T-House (@thouse_opinions), “#Pfizervaccine is not so much about a snap solution for the entire world” (La #Pfizervaccine no es tanto una solución rápida para todo el mundo), Twitter, 10 de noviembre de 2020, 1:34 a. m., https://twitter.com/thouse_opinions/status/1326050492493914112.



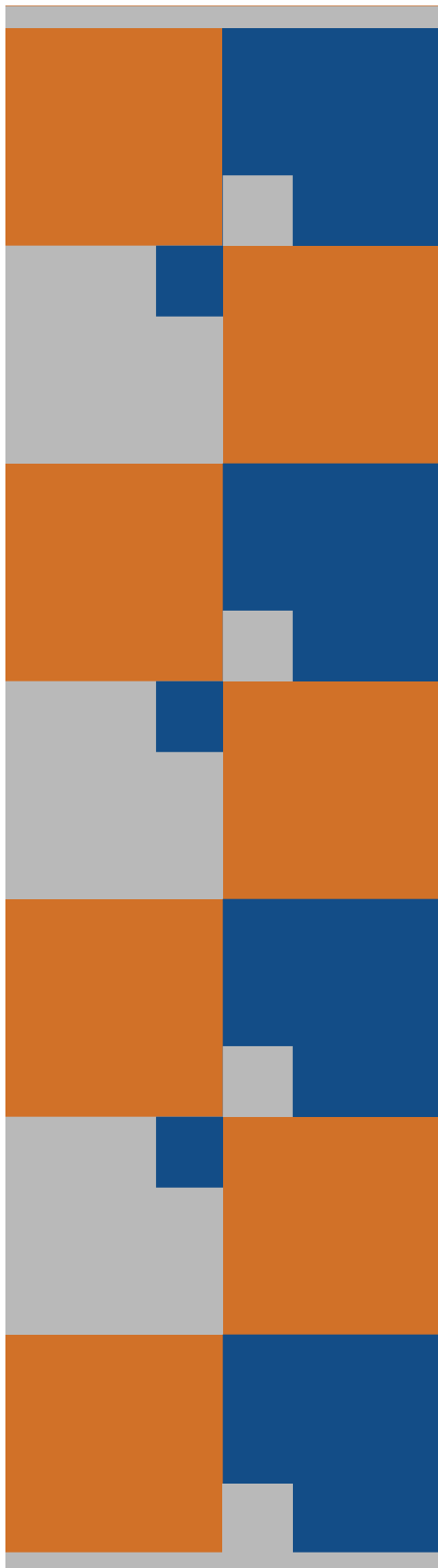
- 12 Anna Nemtsova, “Putin Ramps up RT’s Propaganda Budget as Poll Ratings Slumps” (Putin aumenta el presupuesto de propaganda de RT a medida que las calificaciones en las encuestas se desploman), *The Daily Beast*, 5 de marzo de 2021, <https://www.thedailybeast.com/putin-ramps-up-rts-propaganda-budget-as-poll-rating-slumps>.
- 13 Ibid.
- 14 Bradley Hanlon, “From Nord Stream to Novichok: Kremlin Propaganda on Google’s Front Page” (De Nord Stream a Novichok: la propaganda del Kremlin en la portada de Google), Alianza para asegurar la democracia, 14 de junio de 2018, <https://securingdemocracy.gmfus.org/from-nord-stream-to-novichok-kremlin-propaganda-on-googles-front-page/>; Elen Aghekyan y Bret Schafer, “Deep in the Data Void: China’s COVID-19 Disinformation Dominates Search Engine Results” (En lo más profundo del vacío de datos: la desinformación sobre la COVID-19 de China domina los resultados de los motores de búsqueda), Alianza para asegurar la democracia, 5 de octubre de 2021, <https://securingdemocracy.gmfus.org/data-void-china-covid-disinformation/>.
- 15 Emerson T. Brooking y Suzanne Kianpour, “Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century” (Esfuerzos iraníes de influencia digital: Radiodifusión de guerrilla para el siglo XXI), Atlantic Council, 11 de febrero de 2020, <https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/>; Christopher Bing y Jack Stubbs, “Special Report: How Iran Spreads Disinformation Around the World” (Informe especial: Cómo Irán difunde la desinformación en todo el mundo), *Reuters*, 30 de noviembre de 2018, <https://www.reuters.com/article/us-cyber-iran-specialreport/special-report-how-iran-spreads-disinformation-around-the-world-idUSKCN1NZ1FT>; Michael Barak y Jorge Parades Esteban, “Propaganda, Narratives and Influence in Latin America: Iran, Hezbollah and Al-Tajammu” (Propaganda, narrativas e influencia en América Latina: Irán, Hezbolá y Al-Tajammu), Instituto Internacional contra el Terrorismo (International Institute for Counter-Terrorism, ICT), Universidad Reichman, 3 de julio de 2022, <https://ict.org.il/propaganda-narratives-influence-operations-latin-america/>.
- 16 Jessica Brandt y Bret Schafer, “How China’s ‘Wolf Warrior’ Diplomats Use and Abuse Twitter” (Cómo usan y abusan de Twitter los “guerreros lobo” de la diplomacia china), Institución Brookings, 28 de octubre de 2020, <https://www.brookings.edu/techstream/how-chinas-wolf-warrior-diplomats-use-and-abuse-twitter/>.
- 17 Susanne Oxenstierna y Caroline Vendil Pallin, “*Russian Think Tanks and Soft Power*” (*Think Tanks rusos y poder de persuasión*) (Programa de Rusia en FOI, septiembre de 2017), <https://www.foi.se/rest-api/report/FOI-R--4451--SE>; Ibid.
- 18 Mike Catalini, Amanda Seitz y Eric Tucker, “How China’s TikTok, Facebook Influencers Push Propaganda” (Cómo los influyentes chinos de TikTok y Facebook impulsan la propaganda), The Associated Press, 30 de marzo de 2022, <https://apnews.com/article/china-tiktok-facebook-influencers-propaganda-81388bca676c560e02a1b493ea9d6760>.
- 19 Jessica Brandt, “How the Kremlin Has Weaponized the Facebook Files” (Cómo el Kremlin ha convertido en arma los archivos de Facebook), Institución Brookings, 16 de noviembre de 2021, <https://www.brookings.edu/techstream/how-the-kremlin-has-weaponized-the-facebook-files/>.
- 20 Gaelle Borgia and Michael Schwartz, “How Russia Meddles Abroad for Profit: Cash, Trolls and a Cult Leader” (Cómo se entromete Rusia en el extranjero para obtener beneficios: dinero, trolls y un líder de culto), *The New York Times*, 11 de noviembre de 2019, <https://www.nytimes.com/2019/11/11/world/africa/russia-madagascar-election.html>; Sheera Frenkel y Michael Schwartz, “In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering” (En Ucrania, Rusia pone a prueba una nueva táctica de Facebook para manipular las elecciones), *The New York Times*, 29 de marzo de 2019, <https://seic.myworkfront.com/project/633f39b80010db291aa6c14a2db495d/documents>; Elizabeth Dwoskin, Tony Romm, y Eli Rosenberg, “The Moment When Facebook’s Removal of Alleged Russian Disinformation Became a Free-Speech Issue” (El momento en que Facebook retiró la supuesta desinformación rusa y esto se convirtió en una cuestión de libertad de expresión), *The Washington Post*, 1 de agosto de 2018, <https://www.washingtonpost.com/technology/2018/08/02/moment-when-facebooks-removal-alleged-russian-disinformation-became-free-speech-issue/>.



- 21 Gaelle Borgia and Michael Schwirtz, “How Russia Meddles Abroad for Profit: Cash, Trolls and a Cult Leader” (Cómo se entromete Rusia en el extranjero para obtener beneficios: dinero, trolls y un líder de culto), *The New York Times*, 11 de noviembre de 2019, <https://www.nytimes.com/2019/11/11/world/africa/russia-madagascar-election.html>.
- 22 Jessica Brandt y Amber Frankland, “Leaks, Lies, and Altered Tape: Russia’s Maturing Information Manipulation Playbook” (Filtraciones, mentiras y cintas alteradas: manual de manipulación de la información por parte de Rusia), Alianza para asegurar la democracia, 14 de octubre de 2020, https://securingdemocracy.gmfus.org/russias-maturing-information-manipulation-playbook/#Practicing_tailored_influence.
- 23 Nathaniel Gleicher, “Removing Coordinated Inauthentic Behavior From Russia, Iran, Vietnam and Myanmar” (Eliminación del comportamiento no auténtico coordinado de Rusia, Irán, Vietnam y Myanmar), Meta, 12 de febrero de 2020, <https://about.fb.com/news/2020/02/removing-coordinated-inauthentic-behavior/>.
- 24 C. Shawn Eib et al., “From Russia With Blogs” (Desde Rusia con blogs), Graphika, febrero de 2020, https://public-assets.graphika.com/reports/graphika_report_from_russia_with_blogs.pdf.
- 25 Katie Benner et al., “Saudi’s Image Makers: A Troll Army and a Twitter Insider” (Creadores de imagen saudíes: un ejército de trolls y un infiltrado en Twitter), *The New York Times*, 20 de octubre de 2018, <https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html>.
- 26 Marc Owen Jones, “Qatar Blockade: Saudi-Led Disinformation War Is the Tip of the Iceberg” (Bloqueo de Qatar: la guerra de desinformación dirigida por Arabia Saudita es la punta del iceberg), Middle East Eye, 2 de junio de 2020, <https://www.middleeasteye.net/opinion/qatar-blockade-saudi-led-disinformation-war-just-tip-iceberg>.
- 27 Joe Cheravitch et al., “Combating Foreign Disinformation on Social Media” (Lucha contra la desinformación extranjera en las redes sociales), Rand, 2021, https://www.rand.org/pubs/research_reports/RR4373z1.html.
- 28 Jessica Brandt, Adya Danaditya y Valerie Wirtschafter, “Popular Podcasters Spread Russian Disinformation About Ukraine Biolabs” (Podcasters populares difunden desinformación rusa sobre los biolaboratorios de Ucrania), Institución Brookings, 23 de marzo de 2020, <https://www.brookings.edu/techstream/popular-podcasters-spread-russian-disinformation-about-ukraine-biolabs/>.
- 29 Jessica Brandt y Bret Schafer, “Using the Truth to Tell a Lie: Authoritarian COVID-19 Vaccine Mal-Information Strategies” (Uso de la verdad para decir una mentira: estrategias autoritarias de desinformación sobre la vacuna contra la COVID-19), Power 3.0: Comprensión de la influencia autoritaria moderna, 6 de mayo de 2021, <https://www.power3point0.org/2021/05/06/using-the-truth-to-tell-a-lie-authoritarian-covid-19-vaccine-mal-information-strategies/>.
- 30 David E. Sanger y Nicole Perlroth, “‘Perception Hacks’ and Other Potential Threats to the Election” (Ataques a la percepción” y otras amenazas potenciales para las elecciones), *The New York Times*, 28 de octubre de 2020, <https://www.nytimes.com/2020/10/28/us/politics/2020-election-hacking.html>; Ben Collins, “A Russian Troll Farm Set an Elaborate Social Media Trap for the Midterms” (Una granja de trolls rusos tendió una elaborada trampa en las redes sociales para las elecciones de mitad de mandato), NBC News, 7 de noviembre de 2018, <https://www.nbcnews.com/tech/tech-news/russian-troll-farm-set-elaborate-social-media-trap-midterms-no-n933781>.
- 31 Brandtley Vickery, “Mohammed bin Salman’s ‘Army of Flies’: Saudi Arabia’s Creative Spread of Disinformation and Attack on Political Dissidence” (El ejército de moscas de Mohammed bin Salman: la creativa difusión de desinformación y el ataque de Arabia Saudita a la disidencia política), Democratic Erosion, 30 de noviembre de 2021, <https://www.democratic-erosion.com/2021/11/30/mohammed-bin-salmans-army-of-flies-saudi-arabias-creative-spread-of-disinformation-and-attack-on-political-dissidence/>; Jessica Brandt y Bret Schafer, “How China’s ‘Wolf Warrior’ Diplomats Use and Abuse Twitter” (Cómo usan y abusan de Twitter los “guerreros lobo” de la diplomacia china), Institución Brookings, 28 de octubre de 2020, <https://www.brookings.edu/techstream/how-chinas-wolf-warrior-diplomats-use-and-abuse-twitter/>; Ibid.



- 32 Nate Schenkkan e Isabel Linzer, “*Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression*” (*Ojos que no ven, corazón que no siente: escala y alcance mundiales de la represión transnacional*), (Freedom House, febrero de 2021), https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf.
- 33 Emerson T. Brooking y Suzanne Kianpour, *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century* (*Esfuerzos iraníes de influencia digital: Radiodifusión de guerrilla para el siglo XXI*), (Atlantic Council, 11 de febrero de 2020), <https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/>.
- 34 Freedom House, “Belarus: Freedom on the Net 2021” (Bielorrusia: Libertad en la Red 2021), 2021, <https://freedomhouse.org/country/belarus/freedom-net/2021>.
- 35 Daniel Arnaudo et al., “*Combating Information Manipulation: A Playbook for Elections and Beyond*” (*Lucha contra la manipulación de la información: un manual de estrategias para las elecciones y más allá*), (Instituto Nacional Demócrata, septiembre de 2021), <https://www.ndi.org/publications/combating-information-manipulation-playbook-elections-and-beyond>.
- 36 Jessica Brandt, “How Autocrats Manipulate Online Information: Putin’s and Xi’s Playbooks” (Cómo los autócratas manipulan la información en línea: los manuales de Putin y Xi), *The Washington Quarterly* 44, n.º 3 (2021): 127-154, <https://www.tandfonline.com/doi/abs/10.1080/0163660X.2021.1970902?journalCode=rwaq20>.
- 37 Jessica Brandt, “How Democracies Can Win an Information Contest Without Undercutting Their Values” (Cómo pueden las democracias ganar un concurso de información sin socavar sus valores), Fundación Carnegie para la Paz Internacional, 2 de agosto de 2021, <https://carnegieendowment.org/2021/08/02/how-democracies-can-win-information-contest-without-undercutting-their-values-pub-85058>.
- 38 Jessica Brandt, “How the Kremlin Has Weaponized the Facebook Files” (Cómo el Kremlin ha convertido en arma los archivos de Facebook), TechStream, Institución Brookings, 16 de noviembre de 2021, <https://www.brookings.edu/techstream/how-the-kremlin-has-weaponized-the-facebook-files/>.
- 39 Comité de Derechos Humanos de la ONU, *Comentario general n.º 25: El derecho a participar en asuntos públicos, derecho de voto y el derecho a la igualdad de acceso al servicio público*, reunión n.º 1510, sesión n.º 57 (Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 12 de julio de 1996), <https://www.equalrightstrust.org/ertdocumentbank/general%20comment%2025.pdf>.
- 40 Lucina Di Meco y Kristina Wilfore, “Gendered Disinformation Is a National Security Problem” (La desinformación sexista es un problema de seguridad nacional), TechStream, Institución Brookings, 8 de marzo de 2021, <https://www.brookings.edu/techstream/gendered-disinformation-is-a-national-security-problem/>.
- 41 Comité Digital, de Cultura, Medios de Comunicación y Deporte de la Cámara de Diputados; *desinformación y “noticias falsas”: Informe final* (Parlamento del Reino Unido, 14 de febrero de 2019), <https://publications.parliament.uk/pa/cm201719/cmselect/cmcomeds/1791/1791.pdf>.
- 42 Asamblea General de las Naciones Unidas, *Pacto Internacional sobre Derechos Civiles y Políticos* (Oficina del Alto Comisionado de Derechos Humanos de las Naciones Unidas, 16 de diciembre de 1966), <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.
- 43 “COVID-19 Triggers Wave of Free Speech Abuse” (La COVID-19 desencadena ola de abusos contra la libertad de expresión), Human Rights Watch, 11 de febrero de 2021, <https://www.hrw.org/news/2021/02/11/covid-19-triggers-wave-free-speech-abuse>.



- 44 Jenny Gesley, “Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech” (Alemania: Modificación de la Ley de Aplicación de la Red para Combatir Mejor el Discurso de Odio en Línea), Biblioteca del Congreso, 2021, <https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/>; Ben Wolford, “What is GDPR?” (¿Qué es el RGPD?). GDPR.EU, s.f., [https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU](https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU;); Estrategia Digital de la Comisión Europea, “The Digital Services Act Package” (Paquete de la Ley de Servicios Digitales), Unión Europea, s.f., <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>; Fiscal General de Australia, “Abhorrent Violent Material” (Material Violento Aborrecible), Gobierno Australiano, s.f., <https://www.ag.gov.au/crime/abhorrent-violent-material>.
- 45 Jacob Mchangama y Joelle Fiss, “The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship” (El Muro de Berlín digital: cómo Alemania creó [accidentalmente] un prototipo de censura global en línea) (Justicia, noviembre de 2019), <http://justitia-int.org/en/the-digital-berlin-wall-how-germany-created-a-prototype-for-global-online-censorship/>.
- 46 Lisa Reppell, “Legal and Regulatory Responses to Disinformation” (Respuestas legales y regulatorias a la desinformación), Contrarrestar la desinformación, última modificación el 1 de abril de 2021 <https://counteringdisinformation.org/node/2704/>.
- 47 Adam Satariano, “E.U. Takes Aim at Social Media’s Harms With Landmark New Law” (La UE apunta a los daños de las redes sociales con la nueva ley histórica), *The New York Times*, 22 de abril de 2022, <https://www.nytimes.com/2022/04/22/technology/european-union-social-media-law.html>.
- 48 Grigorij Mesežnikov y Gabriela Pleschová, “Testing Democratic Resolve in Slovakia” (Prueba de resolución demócrata en Eslovaquia), en *Sharp Power: Rising Autocratic Influence* (Fundación Nacional para la Democracia, 5 de diciembre de 2017), <https://www.ned.org/wp-content/uploads/2017/12/Chapter5-Sharp-Power-Rising-Authoritarian-Influence-Slovakia.pdf>.
- 49 Ibid.
- 50 Ministerio del Interior de la República Eslovaca, <https://www.minv.gov.sk/?tlacove-spravy&sprava=ministerstvo-vnutra-aktivne-bojuje-proti-hybridnym-hrozbam-aj-na-europskej-urovni>.
- 51 Seguridad Digital de la Comisión Europea, “Signatories of the 2022 Strengthened Code of Practice on Disinformation” (Firmantes del Código de buenas prácticas en materia de desinformación 2022), Unión Europea, 16 de junio de 2022, <https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation>.
- 52 Franco Luna, “House Bill Seeks Penalties for Creating, Spreading ‘Fake News’” (La Cámara de Representantes sanciona la creación y difusión de noticias falsas), *PhilStar Global*, 8 de agosto de 2022, <https://www.philstar.com/headlines/2022/08/08/2201195/house-bill-seeks-penalties-creating-spreading-fake-news>.
- 53 Oryem Nyeko, “Tanzania Drops Threat of Prison Over Publishing Independent Statistics” (Tanzania retira la amenaza de prisión por publicar estadísticas independientes), *Human Rights Watch*, 3 de julio de 2019, <https://www.hrw.org/news/2019/07/03/tanzania-drops-threat-prison-over-publishing-independent-statistics>.
- 54 “Croatia” (Croacia), *Reporters Without Borders*, s.f., <https://rsf.org/en/country/croatia>; Personal de la Comisión Europea, “2020 Rule of Law Report: Country Chapter on the Rule of Law Situation in Croatia” (Informe del Estado de Derecho de 2020: Capítulo sobre la situación del estado de derecho en Croacia) (Unión Europea, 30 de septiembre de 2020), https://ec.europa.eu/info/sites/default/files/hr_rol_country_chapter.pdf.



- 55 Joe Orovic, “Croatian Gov. in Secret Meeting Urged Media to Fall in Line Ahead of Coronavirus Response” (En una reunión secreta, el gobernador croata instó a los medios de comunicación a alinearse ante la respuesta al coronavirus), *Total Croatia News*, 17 de junio de 2020, <https://www.total-croatia-news.com/news/44353-croatia-government-covid19>.
- 56 Dillon Reisman et al., “Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability” (*Evaluaciones de impacto algorítmico: un marco práctico para la responsabilidad de las agencias públicas*) (Alnow, abril de 2018), <https://ainowinstitute.org/aiareport2018.pdf>; “Algorithmic Impact Assessment: A Case Study in Healthcare” (*Evaluaciones de impacto algorítmico: un estudio de caso en atención médica*) (Ada Lovelace Institute, 8 de febrero de 2022), <https://www.adalovelaceinstitute.org/report/algorithmic-impact-assessment-case-study-healthcare/>.
- 57 Consejo de Europa, <https://rm.coe.int/leaflet-cahai-en-update/1680a23871>.
- 58 Max Fisher, “Disinformation for Hire, a Shadow Industry, Is Quietly Booming” (La desinformación por encargo, una industria en la sombra, está en silencioso auge), *The New York Times*, 25 de julio de 2021, <https://www.nytimes.com/2021/07/25/world/europe/disinformation-social-media.html>.
- 59 Samantha Bradshaw, Hannah Bailey y Philip N. Howard, “Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation” (*Desinformación industrializada: inventario global 2020 de manipulación organizada de redes sociales*) (Programa de Oxford sobre democracia y tecnología, 13 de enero de 2021), <https://www.ox.ac.uk/news/2021-01-13-social-media-manipulation-political-actors-industrial-scale-problem-oxford-report>.
- 60 “Interventions for Ending Online Violence Against Women in Politics” (Intervenciones para poner fin a la violencia en línea contra las mujeres en la política), Instituto Nacional Demócrata, octubre de 2022.
- 61 Access Now et al., “The Santa Clara Principles” (Los Principios de Santa Clara), Los Principios de Santa Clara, s.f., <https://santaclaraprinciples.org>.
- 62 Estrategia digital de la Comisión Europea, “The 2022 Code of Practice on Disinformation” (Código 2022 de buenas prácticas en materia de desinformación), Unión Europea, 16 de junio de 2022, <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>.
- 63 “The GNI Principles” (Principios de la GNI), Iniciativa de Red Global, s.f., <https://globalnetworkinitiative.org/gni-principles/>.
- 64 “Implementation Guidelines” (Pautas de implementación), Iniciativa de Red Global, s.f., <https://globalnetworkinitiative.org/implementation-guidelines/>.
- 65 “OCDE AI Principles Overview” (Descripción general de los principios de IA de la OCDE), IA de la OCDE, mayo de 2019, <https://oecd.ai/en/ai-principles>.
- 66 Jennifer O’Connor, “Building Greater Transparency and Accountability with the Violative View Rate” (Aumentar la transparencia y la responsabilidad con la Tasa de visualización de contenidos infractores), Blog oficial de YouTube, 6 de abril de 2021, <https://blog.youtube/inside-youtube/building-greater-transparency-and-accountability/>.
- 67 Elizabeth Dwoskin, “Facebook Reveals Broad Takedown of Global Disinformation Networks, Including Some Tied to Anti-Vaccine Groups and State Actors” (Facebook revela un amplio desmantelamiento de redes mundiales de desinformación, incluidas algunas vinculadas a grupos antivacunación y actores estatales), *The Washington Post*, 1 de diciembre de 2021, <https://www.washingtonpost.com/technology/2021/12/01/facebook-disinformation-report/>.
- 68 “Google Transparency Report” (Informe de transparencia de Google), Google, última modificación el 2 de junio de 2022, <https://transparencyreport.google.com/?hl=en>.
- 69 Access Now et al., “An Open Letter to Mark Zuckerberg” (Carta abierta a Mark Zuckerberg), Principios de Santa Clara, s.f., <https://santaclaraprinciples.org/open-letter/>.

- 
- 70 *Las plataformas de redes sociales y la amplificación del extremismo nacional y otro contenido perjudicial, ante el Comité de Seguridad Nacional y Asuntos Gubernamentales del Senado de los Estados Unidos*, (26 de octubre de 2021) (testimonio del profesor Nathaniel Persily, el catedrático de derecho James B. McClatchy, codirector del Centro de Políticas Cibernéticas de Stanford, Facultad de Derecho de Stanford) <https://www.dropbox.com/s/r2tgzblora0mayl/Persily%20Senate%20HSGAC%20Testimony.pdf?dl=0>.
- 71 Elizabeth Lange y Doowan Lee, “How One Social Media App Is Beating Disinformation” (Una aplicación de redes sociales combate la desinformación), *Política Exterior*, 23 de noviembre de 2020, <https://foreignpolicy.com/2020/11/23/line-taiwan-disinformation-social-media-public-private-united-states/>.
- 72 Amy Studdart, “Building Civil Society Capacity to Mitigate and Counter Disinformation: Overview – Civil Society” (Fomento de la capacidad de la sociedad civil para mitigar y contrarrestar la desinformación: generalidades – Sociedad Civil), *Contrarrestar la desinformación*, 3 de abril de 2021, <https://counteringdisinformation.org/index.php/topics/csos/0-introduction-building-civil-society-capacity>.
- 73 Ibid.
- 74 Amy Studdart, “Building Civil Society Capacity to Mitigate and Counter Disinformation: Public Awareness/Media Literacy Campaigns” (Fomento de la capacidad de la sociedad civil para mitigar y contrarrestar la desinformación: campañas de concientización pública/alfabetización mediática), *Contrarrestar la desinformación*, 3 de abril de 2021, <https://counteringdisinformation.org/topics/csos/6-public-awarenessmedia-literacy-campaigns>.

Notas

Colofón

© 2022 Instituto Nacional Demócrata para Asuntos Internacionales y Alianza para el Gobierno Abierto

Las publicaciones del NDI y la OGP son independientes de intereses nacionales o políticos específicos. Las opiniones expresadas en esta reseña de políticas no representan necesariamente las opiniones del NDI, la OGP ni las de los miembros de sus respectivas Juntas Directivas.

La versión electrónica de esta publicación está disponible bajo una licencia Creative Commons Attribute-NonCommercial-ShareAlike 3.0 (CC BY-NC-SA 3.0). Algunas partes de este trabajo pueden reproducirse o traducirse para propósitos no comerciales siempre que el NDI y la OGP sean reconocidos como las fuentes de este material y se les hayan enviado copias de cualquier traducción.

Para obtener más información, visite el sitio web de Creative Commons: <http://creativecommons.org/licenses/by-nc-sa/3.0/>

Diseño y disposición: Pamelyn L. Burke