

DESINFORMACIÓN: RIESGOS PARA LA ESTABILIDAD DEMOCRÁTICA EN COLOMBIA

Bogotá, septiembre de 2021

Carlos Augusto Chacón Monsalve

Director Ejecutivo

Instituto de Ciencia Política Hernán Echavarría Olózaga

PRESENTACIÓN

En los últimos años el debate se ha centrado en los riesgos y las amenazas a la estabilidad democrática a causa de fenómenos como las fake news (noticias falsas), información malintencionada o desinformación, en particular, por la amplificación de mensajes e información que están teniendo las redes sociales, así como, la penetración mediante distintos canales de comunicación de países extrarregionales como es el caso de China, Rusia e Irán.

Estos países tienen una característica en común, y la actual coyuntura de tensiones geopolíticas, guerra e incertidumbre global los ponen en evidencia, son los tres principales regímenes autocráticos, con pretensiones revisionistas que buscan confrontar el orden internacional basado en reglas, respeto a la soberanía, los derechos humanos, las libertades individuales y la democracia liberal.

Entre sus estrategias para avanzar en la consecución de sus intereses nacionales, desarrollan operaciones de información y tácticas específicas de desinformación, en el marco de guerras de baja intensidad o de cuarta generación. Su interés es posicionar narrativas y contranarrativas que les permita múltiples objetivos, aprovechando las interacciones, conversaciones y tendencias que se generan en los entornos digitales de las redes sociales.

La desinformación puede perseguir distintos fines, desde legitimar la posición de un régimen autocrático frente a las sanciones económicas internacionales, al tiempo que se utiliza para atacar la legitimidad del Estado o el grupo de Estados que imponen las sanciones.

Por lo tanto, la desinformación consiste en usar información de forma deliberada y sesgada para engañar a la opinión pública sobre un determinado suceso político o fenómeno socioeconómico. De manera intencional se manipulan algunos hechos para posicionar una narrativa que sirva para los objetivos determinados.

Es una táctica que tiene la potencialidad de obtener altos beneficios a bajos costos para el agente que desinforma, pues se vale de la forma en que las redes sociales y algunos medios de comunicación masifican la información y difícilmente se establece la fuente exacta de la cual proviene la desinformación. Se puede considerar como una medida de bajo coste, porque al no existir los medios efectivos para enfrentarla, ya sea mediante la judicialización, las represalias o las sanciones, la recompensa es alta, siempre que contribuya a lograr los intereses estratégicos propuestos.

Recientemente la Unión Europea¹, la OTAN² y los gobiernos de varios países³ han adoptado protocolos para combatir la desinformación y desarrollar capacidades que permitan identificarla de forma oportuna y así, ayudar a la sociedad civil a lograr resiliencia contra esta táctica que busca desestabilizar, atacar la legitimidad de las instituciones, incluidos los procesos electorales, así como minar la confianza de los ciudadanos en sus gobiernos y en los principios y valores democráticos.

¹ Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la manipulación de la información y la desinformación, consideradas como un abuso de las libertades fundamentales de expresión e información, las cuales constituyen una grave violación de los valores y principios democráticos que ambas regiones comparten, los cuales atentan contra la institucionalidad democrática y el Estado de derecho. Se incluyen medidas como: *reforzar la resiliencia mediante la conciencia situacional, la alfabetización mediática y la educación; injerencias extranjeras mediante el uso de plataformas en línea; infraestructuras críticas y sectores estratégicos; injerencia extranjera durante los procesos electorales; financiación encubierta de actividades políticas por donantes extranjeros; ciberseguridad y resiliencia frente a ciberataques; protección de los Estados miembros, instituciones, agencias, delegaciones y misiones oficiales; injerencia por medio de agentes globales a través de la captación de élites, las diásporas nacionales, universidades y actos culturales.* https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_ES.pdf

² En 2022 la OTAN, reconociendo que las amenazas evolucionan en términos de intensidad, objetivos, métodos y medios, establece que el nuevo concepto estratégico de la Alianza debe “brindar la flexibilidad adecuada al diseñar las contramedidas actuales y futuras que guiarán las actividades de la Alianza en los años venideros. En general, la respuesta coherente de la OTAN (y de Occidente) y los esfuerzos contra la desinformación extranjera, tanto a nivel nacional como internacional, deben centrarse en: (i) su resiliencia cívica, (ii) sus capacidades ofensivas tanto como los defensivos y (iii) minimizar las diferencias en cómo los países occidentales individuales abordan la desinformación en la práctica. En otras palabras, la disuasión debe buscarse mediante el castigo y la negación”. Tomasz Chłoń, NATO and Countering Disinformation The Need for a More Proactive Approach from the Member States. GLOBSEC, NATO. 16 de mayo de 2022. <https://www.globsec.org/wp-content/uploads/2022/05/NATO-and-Countering-Disinformation-ver1-spreads.pdf>

³ Taylor, Margaret. Combating disinformation and foreign interference in democracies: Lessons from Europe. Brookings. 31 de julio de 2019. <https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/>

Por esta razón, resulta fundamental entender cómo opera la desinformación y por qué Colombia debe adoptar un marco de política pública y desarrollo normativo para prevenir, enfrentar y disuadir a los actores estatales y no estatales que buscan instrumentalizar la desinformación como una táctica de guerra asimétrica o como un medio de injerencia geopolítica.

EL MARCO DE LA DESINFORMACIÓN

La desinformación constituye un riesgo o amenaza en la medida que puede afectar la legitimidad de las instituciones democráticas y la confianza de los ciudadanos, tanto en el sistema de gobierno, como en el orden internacional vigente.

Esta táctica tiene la potencialidad de diseminarse y amplificarse por parte de actores estatales y no estatales, dentro y fuera del territorio (incluidos actores políticos internos que se benefician de la desinformación), para lo cual, se instrumentalizan distintos canales, ya sean los medios de comunicación tradicionales, las plataformas digitales y las redes sociales.

En cuanto a la desinformación en línea, *“cuando tiene éxito, es un proceso que involucra diferentes actores y etapas consecutivas. Modelamos la desinformación en línea en términos de los malos actores que crean y promueven contenido manipulador, las plataformas que permiten la distribución y promoción de este contenido y las audiencias que le dan significado e impacto a través de su disposición a interactuar con él”*⁴.

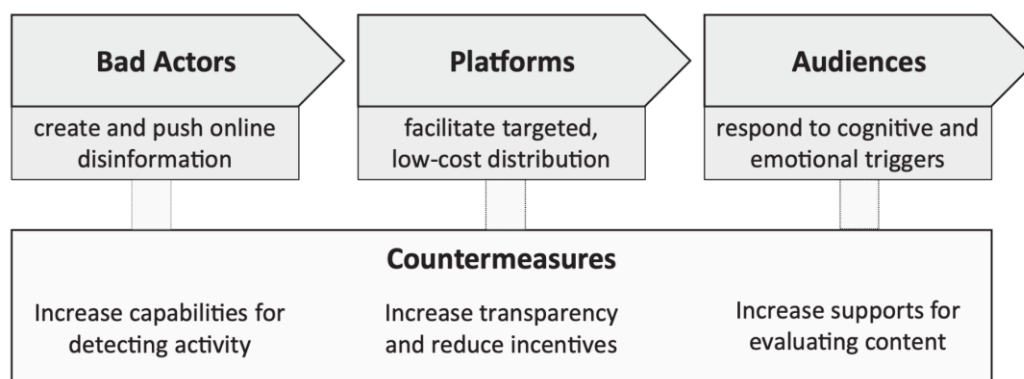


Figura 1.1. El proceso de desinformación. Tomado de *Desinformation and manipulation in digital media: information pathologies*

⁴ Eileen Culloty y Jane Suiter. *Desinformation and manipulation in digital media: information pathologies*. Abingdon, Oxon ; New York, NY : Routledge, 2021. P3.

Los malos actores o los Estados revisionistas no necesariamente tienen que desplegar acciones bélicas convencionales, aunque pueden hacerlo como está sucediendo con la invasión injustificada de Rusia a Ucrania para buscar objetivos estratégicos e infligir daño a sus adversarios. El dominio de la información se ha convertido en un teatro de operaciones que permite a estos actores y sus proxies no estatales llevar a cabo campañas de desinformación y ciberataques para desestabilizar países y socavar la institucionalidad democrática, influyendo en el proceso de toma de decisiones de los ciudadanos mediante la manipulación de la información.

En el marco de la pandemia de la COVID-19 se pudo evidenciar la forma en que Rusia y China usaron la desinformación: *“El Kremlin, el PCCh y sus aliados han explotado la viralidad de las redes sociales y la incapacidad de los ciudadanos para pensar críticamente sobre la información que consumen para crear y amplificar contenido falso a nivel mundial. Durante la pandemia, compartir falsedades cuesta vidas. En respuesta a este desafío masivo, las plataformas digitales han intensificado sus esfuerzos para contrarrestar la desinformación y la información errónea sobre el COVID-19”*⁵.

La injerencia de los Estados autócratas también opera mediante la captura de élites políticas⁶, de opinión y académicas, y de otros entornos que permitan generar confianza y dar legitimidad a las narrativas que hacen parte de las acciones de desinformación.

El Comité Especial sobre Interferencia Extranjera en todos los Procesos Democráticos en la Unión Europea, incluida la Desinformación (INGE, por sus siglas en inglés) encontró una falta de concienciación sobre los riesgos de la interferencia extranjera maligna en la democracia y la sociedad europea y adoptó sus recomendaciones finales de enero de 2022 después de 18 meses de investigación⁷.

⁵ Vera Zakem, Edward Lucas y James Lamond. Owing the Conversation Assessing Responses to Russian and Chinese Information Operations Around COVID-19. The Center for European Policy Analysis (CEPA). 31 de marzo de 2022. <https://cepa.org/owning-the-conversation-assessing-responses-to-russian-and-chinese-information-operations-around-covid-19/>

⁶ Se pueden citar dos casos de estudios específicos: 1. La captura de élites políticas alemanas por parte de Rusia: Jeffrey Mankoff. With Friends Like These. Assessing Russian Influence in Germany. Elite Capture. Center for Strategic and International Studies (CSIS) (2020) <https://www.istor.org/stable/resrep25324.5> 2. Un presunto intento de captura de élites del Reino Unido por parte de China: Larisa Brown. The Daily Mail. Julio de 2020. Trump dirty dossier spy reveals how China 'targets British VIPs': Former MI6 spy Christopher Steele accuses Beijing of grooming UK establishment figures to be 'full-time agents' or 'useful idiots'. <https://www.dailymail.co.uk/news/article-8495775/Former-MI6-spys-dossier-sparks-Huawei-storm-useful-idiots-claims.html> y The curious case of the Huawei dossier A dossier claiming that China orchestrated a campaign to enlist the support of British politicians was leaked last week, but who is behind it? Lauri Clarke. New Statesman. Julio 2020. <https://www.newstatesman.com/politics/uk-politics/2020/07/curious-case-huawei-dossier>

⁷ Andreas Rogal. El Parlamento Europeo pide a la UE que refuerce las defensas contra la desinformación y la captura de élite. The Parliament Magazine. <https://www.theparliamentmagazine.eu/news/article/european-parliament-calls-on-eu-to-strengthen-defences-against-disinformation-and-elite-capture>

Para desarrollar y posicionar el relato recurren al revisionismo histórico, buscando justificar las guerras, las violaciones a los derechos humanos y restricciones a la libertad, con el fin de legitimar sus acciones tanto a nivel interno como externo. Mediante la desinformación se impulsan imaginarios que les permite crear una percepción en la matriz de opinión sobre sus causas, y en muchos casos, sobre la superioridad moral de sus regímenes autoritarios sobre las democracias liberales, al señalarlas de poco efectivas, injustas e ilegítimas.

Los regímenes autoritarios promueven la desinformación puesto que cuentan con la capacidad de crear y promover abundantes narrativas que, siendo demostrablemente falsas, pueden ser plausibles porque mezclan verdades con mentiras, tergiversan la información, los datos y los hechos.

Las operaciones de información se desarrollan usando tácticas de desinformación aprovechándose de las sociedades abiertas y la libertad de expresión. Esto porque su apertura y pluralismo llegan a constituir una vulnerabilidad estratégica, toda vez que, el flujo masivo de información permite diseminar relatos falsos y crear narrativas sobre “conspiraciones” que se hacen virales. De forma tal que se pueda afectar la participación política, induciendo al error y al engaño de los ciudadanos para afectar su comportamiento electoral⁸, convirtiendo a los electores en un objetivo de ataques de desinformación.

Un caso documentado fue la desinformación promovida por Irán en el marco del proceso electoral de Estados Unidos en 2020. Irán, a través de diversos agentes envió correos electrónicos falsificados a miles de votantes estadounidenses en Florida, Alaska y Arizona, haciéndose pasar por un grupo extremista de derecha, amenazaban con perseguir a los destinatarios si no votaban por el entonces presidente Donald Trump. Este caso puso de manifiesto la forma en que Irán utiliza la desinformación como represalia: *“La temeraria incursión de Irán en la interferencia electoral de EE. UU. puede haber sido una señal de la creciente desesperación de Irán por escapar de la campaña de máxima presión montada por la administración Trump apoyando a un candidato opositor que creía que sería un adversario menos agresivo y más predecible.*

⁸ “El contexto estratégico que falta es que Estados Unidos se encuentra actualmente en una guerra no cinética con Rusia e Irán en la que los votantes estadounidenses son el objetivo. No sabemos qué va a hacer Rusia con sus copias de las listas de votantes estadounidenses. La última operación cibernética de Irán no es todo lo que Irán es capaz de hacer. Irán tiene el potencial de sorprendernos en el ciberespacio. Y Rusia ciertamente puede hacerlo peor”. Thomas S. Warrick. How to defeat Iranian and Russian cyber operations against the US election. Atlantic Council. 28 de octubre de 2020. <https://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-defeat-iranian-and-russian-cyber-operations-against-the-us-election/>

Apenas unos días antes de la estafa por correo electrónico, la administración Trump volvió a imponer severas sanciones a Irán, incluso a su sector financiero”⁹.

En los últimos meses en América Latina se ha evidenciado la forma como se utiliza la desinformación para desacreditar a las instituciones, para minar la confianza de los ciudadanos e incitar al malestar social, que ha derivado en manifestaciones violentas, que llevaron a cambios políticos en varios países de la región, en particular Chile y Colombia.

Como lo destaca el Center for a Secure Free Society, en su reporte *Asalto Asimétrico a Colombia* “en un estudio de 7,6 millones de interacciones digitales, se encontraron vinculaciones con las protestas de Colombia y Chile de 2019, los analistas forenses digitales encontraron que menos del 1 por ciento de los usuarios generaban casi el 30 por ciento del contenido, con la mayoría de las cuentas geolocalizadas en Venezuela. Otro estudio encontró que 4.8 millones de tweets entre el 20 de octubre y el 5 de noviembre de 2019, de un gran grupo de hashtags a favor de las protestas en Chile, se originaron en Venezuela, Nicaragua y Cuba”¹⁰.

La desinformación, como táctica de penetración, también hace parte de estrategias de injerencia. El Instituto de Ciencia Política Hernán Echavarría Olózaga con el apoyo del DT Institute de Estados Unidos, ha analizado con distintos expertos a través de una serie de Podcast¹¹, la forma en que Irán utiliza la desinformación en América Latina y el Caribe para legitimarse en la región y justificar su lucha contra Occidente, crear identidades revisionistas y revolucionarias con sectores políticos latinoamericanos antiestadounidenses, reclutar operativos mediante los centros culturales islámicos, buscar apoyos internacionales para lograr un acuerdo nuclear, cuestionar y evadir las sanciones impuestas por Estados Unidos, y exculpar su responsabilidad frente a los atentados de la AMIA en Argentina en 1994. De igual forma, facilitar la penetración y la creación de redes criminales por parte de Hezbollah en regiones como la Triple Frontera, Venezuela, Perú, Bolivia, Brasil y Argentina.

⁹ Sonja Swanbeck. How to Understand Iranian Information Operations. Lawfare. 19 de febrero de 2021. <https://www.lawfareblog.com/how-understand-iranian-information-operations>

¹⁰ HUMIRE Joseph. Asalto Asimétrico a Colombia. Secure Free Society. 19 de mayo de 2021. <https://www.securefreesociety.org/research/asalto-asimetrico-a-colombia/>

¹¹ 1. Soleimani: ¿Héroe, revolucionario o criminal de guerra? <https://youtu.be/O9zKaX2RX3U> 2. ¿Es seguro el mundo con un Irán nuclear? <https://youtu.be/5H9IM7E8aUQ> 3. ¿Es Irán un aliado internacional influyente en América Latina y Colombia? <https://youtu.be/Vqt6REWljbM> 4. ¿Qué hay detrás de la trama del avión de Emtrasur varado en Argentina? <https://youtu.be/RfpkMAIvYNU> 5. La influencia de Irán en Perú <https://youtu.be/gMZuk0nnJmk> 6. Un nuevo acuerdo nuclear con Irán <https://youtu.be/JAPnEfXnx2I>

LOS RETOS FRENTE A LA DESINFORMACIÓN COMO AMENAZA A LA DEMOCRACIA Y LA SEGURIDAD

Entendiendo las implicaciones de un fenómeno complejo y multicausal, en el que pueden actuar agentes estatales como no estatales, tanto regionales como extrarregionales, es necesario que se defina un concepto estratégico que permita diseñar cursos de acción efectivos, legítimos, integrales y coherentes. Para esto, resulta indispensable determinar si se cuenta con los medios para detectar y prevenir la captación de élites políticas, académicas y de opinión para ponerlos en evidencia cuando gestionan intereses de regímenes autoritarios. Además, es necesario contar con medios efectivos para contrarrestar el establecimiento de canales de influencia dentro de organizaciones públicas y privadas.

Diferentes países y organizaciones multilaterales reconocen los riesgos y amenazas que implican las tácticas de desinformación, para lo cual, han definido estrategias, planes, programas, proyectos y protocolos que mitiguen su impacto, gestionen el riesgo y enfrenten a los responsables de esta práctica.

Es preciso que además de reconocer el problema se desarrollen capacidades que permitan:

1. Formar a la sociedad civil e informar a la opinión pública y tomadores de decisión sobre la desinformación para generar conciencia situacional y resiliencia social.
2. Diseñar protocolos de contrainteligencia y contramedidas frente a la desinformación.
3. Establecer mecanismos de cooperación con terceros países y a nivel multilateral, especialmente para la transferencia de conocimientos, tecnologías y buenas prácticas¹².
4. Diseñar e implementar medidas de disuasión contra los Estados promotores y patrocinadores de la desinformación y sus agentes locales.

¹² En este aspecto la cooperación se puede orientar a países que llevan años enfrentando la desinformación y han desarrollado capacidades propias como es el caso de Estonia y República Checa. Countering Russian Disinformation. Center for Strategic and International Studies. 23 de septiembre de 2020. <https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation>

5. Invertir en recursos tecnológicos y capital humano que permitan crear un ecosistema y la infraestructura necesaria para la verificación de datos e identificación de actores y formas, incluida la denominada desinformación por contrato¹³.
6. Definir un régimen de sanciones contra responsables, publicar nombres de los agentes, de sus patrocinadores y financiadores.
7. Desarrollar marcos normativos y estándares sobre desinformación e integridad de la información para las campañas electorales.
8. Invertir en la investigación independiente a través de Universidades y Centros de Pensamiento (Think Tanks) para generar conocimiento y comprender las dinámicas de la desinformación, sus responsables, objetivos, el ecosistema en el que operan y los impactos que generan.

¹³ “En lugar de actores individuales, la regulación debe pensar en términos de redes de comunicación, cadenas de valor y soluciones neutrales desde el punto de vista tecnológico y de contenido. Se debe interrumpir la lucrativa cadena de valor de generar desinformación y se deben desarrollar mejor las prácticas ya conocidas de desmonetización. Por ejemplo, las firmas de relaciones públicas que han comenzado a especializarse en campañas de desinformación deberían enfrentar restricciones legales e incluso sanciones. Al mismo tiempo, los medios de comunicación de calidad en apuros deberían estar mejor organizados y financiados. Deben crearse cadenas de producción y distribución de contenido de confianza y redes de colaboración, y debe establecerse una verificación cruzada de los hechos entre los miembros de la red, así como un protocolo similar a una cadena de bloques que verifique la autenticidad del contenido a lo largo de su cadena de distribución, incluido el intercambio”. Judit BAYER, Bernd HOLZNAGEL, Katarzyna LUBIANIEC, Adela PINTEA, Josephine B. SCHMITT, Judit SZAKÁCS, Erik USZKIEWICZ. Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States. Policy Department for External Relations Directorate General for External Policies of the Union. Abril de 2021. [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653633/EXPO_STU\(2021\)653633_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653633/EXPO_STU(2021)653633_EN.pdf)