LA DESINFORMACIÓN DE NUEVA GENERACIÓN
Cinco escenarios políticos y geoestratégicos ante el *fake*

CARME COLOMINA,
Investigadora CIDOB

Vivimos en realidades confusas. En mundos polarizados que alimentan el choque de relatos. Los intentos de manipulación no tienen límites geográficos ni un único origen. Pueden proceder de esfuerzos patrocinados por determinados estados, o ser un instrumento de las estrategias de individuos o grupos motivados por promover una visión particular del mundo, por un interés económico o, simplemente, puede que no tengan *más* objetivo que la desestabilización a través de la disrupción y el caos. La postverdad actual ya no responde únicamente a un desafío ideológico. También puede que no pretenda confrontar modelos sino, simplemente, contribuir a la confusión. La mentira es ruido. La información distorsionada no siempre busca convencer, sino más bien enfatizar divisiones y erosionar los principios de confianza compartida que deberían cohesionar las sociedades. Las posibilidades de difusión e influencia que brindan las redes sociales y los ingresos por publicidad son solo una parte de la historia de la desinformación. Organizaciones, gobiernos y poderes establecidos deberían preguntarse también ¿por qué las noticias falsas encuentran una audiencia tan receptiva?

Vivimos en un tiempo caracterizado por un creciente desencanto y por la desconfianza en las instituciones gubernamentales. En esta era del "contra–conocimiento" –como lo define el periodista y editor Damian Thompson– donde la "(des)información es empaquetada para que parezca un hecho", la verdad es cuestión de percepciones.

La transformación tecnológica conlleva la transformación política y social. Nos ha cambiado el concepto de poder, la idea de amenaza y los escenarios de confrontación. Si los cambios provocan sensación de inseguridad, la evolución continua de los medios de comunicación –y, en consecuencia, el futuro de la desinformación– puede seguir aumentado este sentimiento de desasosiego que se traduce en volatilidad electoral.

Estamos enseñando a las computadoras no solo a leer, a analizar y a hablar, también las hemos programado para combinar todas estas informaciones, para reconocer y emplear emociones y para generar todo tipo de contenido. Nuestra relación con la tecnología está a punto de dar un nuevo vuelco hasta aumentar aún más nuestra vulnerabilidad a la erosión de la privacidad y a la exposición masiva de nuestros datos personales.

¿De qué manera se está configurando el futuro inmediato de la desinformación? ¿Qué estrategias, instrumentos, percepciones o intenciones políticas están determinando la respuesta de gobiernos e individuos ante estas nuevas vulnerabilidades? Seis grandes tendencias marcan el momento actual del análisis político y el desarrollo tecnológico de la desinformación:

1 – Atrapados en el año 2016

La desinformación siempre va un paso por delante. Los avances tecnológicos preceden cualquier medida o legislación que pretenda regular sus efectos. La línea divisoria entre propaganda e información es cada vez más borrosa, también en las democracias occidentales. La irrelevancia de la verdad factual sigue aumentando en cada nuevo escenario electoral y las vías de transmisión de las falsedades se sofistican. Sin embargo, el debate político sobre la amenaza de la desinformación y como combatirla sigue anclado en el 2016, en los precedentes del referéndum del Brexit y las elecciones presidenciales estadounidenses como referencia y medida de todas las cosas; con la desinformación rusa como principal amenaza reconocida por la Unión Europea y el abuso del término "*fake news*" como arma de descrédito del discurso crítico y el disenso político. Pero, la realidad actual es ya mucho más compleja.

El uso de la (des)información en la acción política se ha trasladado desde las redes sociales y las plataformas abiertas a los espacios digitales cerrados y de confianza como los grupos de WhatsApp. Ello obliga a repensar estrategias para adaptarse a unos parámetros legales, tecnológicos y éticos distintos. La desinformación está en plena evolución desde el texto escrito a las imágenes y sigue sofisticándose por momentos mientras gobiernos –especialmente en la Unión Europea– constatan la imposibilidad de consensuar visiones y estrategias. Las percepciones y evaluaciones de riesgo del fenómeno siguen tomándose bajo prismas nacionales cuando el desafío es global.

La desinformación que desestabiliza el debate democrático en la UE no es únicamente una amenaza exterior sino que se construye, coordina y re–elabora su retórica anti–europea, desde el interior, apoyada en campañas euroescépticas gubernamentales y amplificada por las estrategias mediáticas de distintas formaciones políticas europeas. La desinformación a través de Whatsapp ha hecho acto de presencia en las últimas elecciones generales españolas, a unos niveles todavía nada comparables a sus efectos en países como Brasil o India, pero apunta ya hacia una tendencia que se extiende mucho más allá de la estrategia política comunitaria para intentar atajar los efectos de las narrativas falsas en la configuración de las opiniones políticas de sus ciudadanos.

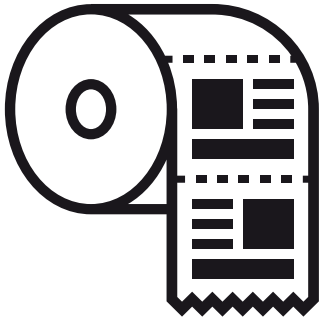
2 – Regulación o censura

El debate sobre cómo combatir las noticias falsas colisiona con el derecho a la libertad de expresión. ¿Cómo puede la Unión Europea atacar un problema que se percibe con grados diferentes de preocupación entre sus estados miembros y que se aborda desde enfoques legislativos distintos?

El parlamento alemán aprobó una ley para multar a las plataformas de internet y a las redes sociales con más de dos millones de usuarios que no erradiquen contenido denunciado como falso o como discurso del odio. Francia, en cambio, ha preferido dotar a los tribunales de capacidad de decisión sobre la exactitud de la información en línea que se publique durante los procesos electorales. Estados Unidos, por su parte, propuso una legislación para aumentar la transparencia sobre quién compra anuncios (políticos) en las redes sociales. Italia y Suecia han introducido la formación en competencia digital en las escuelas para mejorar la detección y la lectura crítica de noticias falsas y de la propaganda. El objetivo general es fortalecer la capacidad de resiliencia de los europeos ante el desconcierto de la desinformación. Pero, a la vez, demuestra la variedad de aproximaciones legales y políticas al fenómeno.

Por su parte, la Unión Europea optó por un Código de Prácticas, aprobado en el 2018, que ambicionaba sumar a las grandes plataformas de internet (Google, Facebook, Twitter o Mozilla) en la intensificación del control sobre el contenido que circula en la red, la eliminación de cuentas falsas y la limitación de la visibilidad de páginas consideradas promotoras de desinformación. Sin embargo, el hecho de que estas plataformas deban actuar ahora como si fueran los reguladores de la veracidad de los contenidos, ha provocado conflictos de intereses con los políticos que habitualmente usan las redes sociales para compartir su propio contenido sesgado, tensiones con partidos tradicionales que han visto algunas de sus cuentas suprimidas durante períodos electorales, y acusaciones de que las *Big Tech* restringen el discurso político legítimo. Para los más críticos, dotar a las plataformas de autoridad para retirar contenido las habilita para actuar como censores, incluso cuando algunas de estas redes sociales han mostrado dificultades evidentes para pronunciarse sobre qué consideran o no una noticia falsa.

La información distorsionada no siempre busca convencer, sino más bien enfatizar divisiones y erosionar los principios de confianza compartida que deberían cohesionar las sociedades



En este escenario de *privatización* de la censura, las grandes plataformas son ahora, en realidad, juez y parte. Acumulan un control sin precedentes de datos y comportamientos individuales y una concentración masiva de los intercambios comunicativos que se producen a través de las redes sociales. La cuota de mercado global de Google es del 80% de todas las consultas de búsqueda que se realizan en internet, mientras Facebook y YouTube controlan el 70% de las interacciones en redes sociales. ¿Cómo se puede responder a esta concentración de poder y datos?

El discurso acusador está claro. La respuesta, no. ¿Cómo consensuar estrategias entre distintos intereses geopolíticos con distintos instrumentos legales o securitarios? El poder de la desinformación y la sofisticación tecnológica no solo se perciben como un desafío también se han configurado como una oportunidad para el control social y la represión ideológica. Mientras se debate como abordar las crecientes preocupaciones sobre la privacidad, las nuevas tecnologías están dotando a los gobiernos de un poder sin precedentes para controlar, seguir y vigilar a sus ciudadanos. Armados con esta información, cualquier corporación, gobierno o actor no–estatal puede desplegar una campaña disruptiva que difunda contenido dirigido a incitar una respuesta emocional.

Según el informe *Freedom of the Net 2017*, gobiernos de hasta 30 países distintos, entre ellos Turquía, Venezuela o Filipinas, producen y difunden contenidos con el fin de distorsionar la información que circula en internet. El gobierno chino se ha convertido en un *gran hermano* capaz de monitorizar los movimientos de sus ciudadanos a través de teléfonos móviles. Organizaciones de derechos humanos han denunciado las legislaciones contra las *fake news* aprobadas en Egipto o Gambia como un ataque a la libertad de expresión. La Ley para la Protección contra la Falsedad y la Manipulación *online* aprobada por el gobierno de Singapur es la más dura de todas las medidas adoptadas en el Sudeste Asiático y una amenaza directa a la libertad de prensa y de expresión, con multas millonarias y hasta diez años de cárcel que pretenden criminalizar, no solo la mentira, sino la crítica al gobierno y la disidencia política.

3 – El impacto de la postverdad en el multilateralismo

La geopolítica de la postverdad ha transformado amenazas y estrategias. Rusia y China han tomado la iniciativa para intentar establecer estrictas leyes de ciberseguridad que les permitan mantener un mayor control sobre el flujo de información en la red para salvaguardar los intereses nacionales. Mientras Moscú y Beijing pactan priorizar su cooperación en materia de seguridad, la Unión Europea sigue atrapada en la conciencia de su propia vulnerabilidad.

Shoigu, ya había admitido un año antes que, desde el 2013, su ministerio albergaba una unidad especializada en la guerra de información.

Rusia es un adversario híbrido para una Unión Europea que no se puede plantear competir por la hegemonía en el ciberespacio. En la última Estrategia Global de la UE, del 2016, Rusia pasó de ser considerada un "socio estratégico" a figurar como "amenaza estratégica", dispuesta a debilitar a su adversario –atacando su cohesión interna y erosionando sus instituciones– con medios no convencionales.

tribuir a su desestabilización. El ciberespionaje no solo por motivos de seguridad sino también económicos es una de las acusaciones recurrentes que pesan sobre el gobierno chino. La aceleración tecnológica china ha revolucionado los equilibrios globales y plantea nuevos choques geoestratégicos. El último de los cuales se ha traducido en una guerra comercial, de reglas internacionales y de acusaciones de espionaje contra el gigante chino de teléfonos y tabletas Huawei. La administración Trump ha ejercido presión sobre países de todo el mundo para que no utilicen los equipos de Huawei en el desarrollo de redes 5G de próxima

La utilización masiva del *Big Data* dejó desprotegidos a millones de europeos. En marzo de 2018 salió a la luz el escándalo de Cambridge Analytica, la consultora que utilizó, sin permiso, los datos personales de 87 millones de usuarios de Facebook –2,7 millones de los cuales eran ciudadanos de la Unión Europea–.

Ese mismo mes, el ataque con gas nervioso contra el ex espía ruso Sergei Skripal y su hija en suelo británico se tradujo en nuevas sanciones contra Rusia (que se sumaban a las ya aprobadas en el 2017 contra la interferencia electoral rusa en las elecciones presidenciales norteamericanas). Esta vez, Estados Unidos incluyó en su lista a 16 entidades e individuos vinculados a la Agencia de Investigación de Internet (Internet Research Agency), con sede en San Petersburgo, considerada una *fábrica de trolls* dedicada a producir y diseminar contenido disruptivo a través de las redes sociales. El ministro de Defensa ruso, Sergey

También en el 2017, el *Munich Security Report* afirmó que la postverdad tiene una clara dimensión de seguridad: si los políticos mienten, "¿pueden los ciudadanos y sus aliados confiar en ellos en temas de seguridad nacional?" Algunos observadores han advertido que la diplomacia multilateral también corre el riesgo de caer en una realidad en la que los diplomáticos no estén de acuerdo con hechos básicos ni crean en la palabra del otro ante los compromisos de seguridad adquiridos. La misma preocupación ha llegado a la sede de Naciones Unidas alarmada por los efectos de una combinación letal entre el menosprecio creciente a los derechos humanos y la erosión de la confianza institucional y del método multilateral por parte de grandes potencias y, especialmente, de los Estados Unidos.

Por su parte, China se ha servido de los ciberataques contra países con los que mantiene disputas territoriales regionales, desde Filipinas, a Vietnam, Taiwan, Malasia o Brunei, para con-

generación, asegurando que los productos de la empresa china representan un riesgo para la seguridad.

4 – El orden algorítmico

Los algoritmos controlan en gran medida la predeterminación selectiva de la información que vemos. Así, aquellos que deciden la previsibilidad de lo que consumimos consolidan su poder sobre nosotros. Los algoritmos nos mostrarán el mundo que, según sus cálculos, deberíamos querer ver. Es la *ciber–balcanización* de las preferencias, incluidas las afiliaciones sociales, intelectuales y económicas, –según el término acuñado por Marshall van Alstyne y Erik Brynjolfsson en un estudio sobre la *comunidades electrónicas* (1997)– que nos sumergen en microcomunidades autoreferenciales, en silos de verdades distintas, sólo compartidas por aquellos que se nos asemejan.

Los bots, por su parte, están diseñados para amplificar el alcance no solo de los mensajes políticos, también de las noticias falsas y explotar así las vulnerabilidades que surgen de nuestros sesgos cognitivos y sociales.

Cambiar la configuración de los algoritmos para reducir la importancia de algunos contenidos, como se plantea en algunos casos, podría convertirse en una trampa contra la libre circulación de la información. Se reduciría probablemente la cantidad de contenido falso en la red pero, a la vez, también reduciría el número de "noticias reales" y, por tanto, no mejoraría los estándares de calidad de la información al alcance de los usuarios. Una vez más, sin embargo, los expertos señalan hacia el poder de las plataformas en la configuración de la esfera pública. "Twitter es un motor, no una cámara", asegura el profesor Evgeny Morozov de la Universidad de Stanford. La mediación algorítmica y la dieta informativa (o desinformativa) que nos impone, en forma de microclimas de opinión, se determina de forma unilateral desde las grandes plataformas de internet.

5 – La carrera por la Inteligencia Artificial

En octubre del 2018, Microsoft admitía que estaba dispuesta a vender el Pentágono a cualquier sistema de inteligencia artificial que necesite para "construir una defensa fuerte". Hoy por hoy, sin embargo, Beijing y Moscú emergen como las grandes potencias del ciberespacio. Sin tratados que las limiten.

En países autoritarios –y en más de una democracia liberal–, los sistemas de inteligencia artificial contribuyen al control y la vigilancia de sus ciudadanos, dotando a las fuerzas de seguridad de grandes cantidades de información que podrá ser procesada de manera rápida y eficiente. Un mundo orwelliano con cámaras de reconocimiento facial y tomas obligatorias de muestras de ADN. Sistemas de vigilancia en Xinjiang o en el Tibet, construcciones de ciudades inteligentes por parte de gigantes tecnológicos chinos, como Huawei, en países terceros y la exportación de sistemas de vigilancia avanzados a países aliados al servicio de la estrategia geopolítica.

Sin embargo, vale la pena destacar algunos movimientos en sentido contrario. La alcaldía de la ciudad de San Francisco, en Estados Unidos, ha prohibido recientemente a la policía local el uso de técnicas de reconocimiento facial,

criticadas por las organizaciones pro derechos civiles. Con ello, pretenden abrir el debate sobre la responsabilidad en torno a la tecnología de la vigilancia en un país donde las agencias de seguridad gubernamentales han promovido el espionaje masivo de ciudadanos nacionales y extranjeros, y la policía se ha visto envuelta en reiterados episodios de sesgos raciales y étnicos, que estas tecnologías de reconocimiento multiplican. También en el Reino Unido, un ciudadano británico denunció, en mayo del 2019, al departamento de policía del sur de Gales ante los tribunales por el uso indiscriminado y sin regulación legal de la tecnología de reconocimiento facial automático.

La línea divisoria entre propaganda e información es cada vez más borrosa, también en las democracias occidentales

En China, en cambio, ya hay casi 200 millones de cámaras y el gobierno está decidido a erigirse en una potencia de la Inteligencia Artificial para el año 2030. La compañía Yitu Technology está desarrollando un programa de reconocimiento que permitiría incluso la lectura de las emociones. Tecnología al servicio del control del entorno más próximo y del espacio virtual. Detrás de esta voluntad hay una estrategia económica y política desplegada desde hace años. En el 2004, un documento de Defensa Nacional del gobierno chino ya especificaba que la información se había convertido "en un factor clave para aumentar la capacidad militar efectiva de las Fuerzas Armadas". El "ciberespacio es hoy el nuevo terreno de confrontación en la contienda militar", rezaba un estudio de la Academia de Ciencias Militares china en el 2013.

El ciberespacio es una cuestión de seguridad nacional para Beijing y, sobre esta premisa, ha desarrollado su estrategia de respuesta: desde la monitorización del contenido en internet y en las redes sociales, con la construcción de su propia "Gran Muralla" virtual susceptible de controlar un posible malestar social al desarrollo de su propia infraestructura y en su estrategia de "Defensa activa".

6 – *Deepfake*, el fin del "ver para creer"

La Inteligencia Artificial también está al servicio de la desinformación. Es el *deepfake*: algoritmos al servicio de la creación de audios y vídeos falsos, desvirtuando todavía más la ya diluida frontera entre realidad y ficción.

Hace dos años, la Universidad de Washington presentó un proyecto piloto conocido como *Synthesizing Obama*, un algoritmo capaz de manipular vídeos sincronizados con movimientos faciales que usaba la imagen del expresidente de Estados Unidos, Barack Obama, para reproducirla en contextos distintos repitiendo la misma declaración. ¿Cuál de ellas era la auténtica?

Recreaciones faciales, construcciones de discursos a partir de la manipulación de intervenciones o alocuciones grabadas previamente, capacidad de reproducir idénticamente expresiones faciales... una nueva generación de manipulaciones está a punto de irrumpir en el caos de la desinformación. Las implicaciones políticas y securitarias de esta tecnología son obvias: cualquier líder político podría aparecer diciendo o haciendo cualquier movimiento o anuncio con consecuencias estratégicas y que, en realidad, se trate de un montaje. Una ficción fabricada para la desestabilización política.

Nuevas formas de amenazas híbridas podrían aparecer en un futuro próximo en otros países y zonas del planeta. Internet es el nuevo territorio geoestratégico y la tecnología, el campo donde se decide la próxima hegemonía global. Washington y Beijing están en pleno desafío por su control.