Desinformación: concepto y perspectivas

Julia Alicia Olmo y Romero | Embajadora en Misión Especial para las Amenazas Híbridas y la Ciberseguridad. Ministerio de Asuntos Exteriores, Unión Europea y Cooperación.

Tema

La desinformación, cuando responde a una estrategia y unos objetivos de desestabilización, pone en riesgo los valores e instituciones democráticos, como los de la Unión Europea, ya erosionadas por conceptos como la posverdad, las fake news y la manipulación de las redes sociales.

Resumen

La desinformación está de plena actualidad. Ha entrado de lleno y con fuerza en la vida política, económica y social, en nuestra esfera privada y en nuestro lenguaje habitual. Es un término cuyo concepto aparece asociado a otros, como *posverdad*, *ciberseguridad* o *injerencias*, también de actualidad (baste pensar en que el diccionario Oxford declaró *post-truth* palabra del año 2016 y que en 2017 volvió a hacer lo mismo con *fake news*). Este ARI analiza esos conceptos y otros afines para explicar cómo se pueden ver en peligro las instituciones y valores democráticos de la Unión Europea si no se toma a tiempo conciencia de la desinformación y se genera una resiliencia democrática.

Análisis

Posverdad: fetichismo y mentira

Detengámonos primero en el concepto de posverdad. Un concepto que ya estaba en la mente del dramaturgo serbio-estadounidense Steve Tesich, que en 1992 la utilizó en la revista *The Nation* en referencia al escándalo Irán-Contra para mostrar la predisposición de la opinión pública a admitir las mentiras de sus gobernantes. Lo siguieron Ralf Keyes[1], Eric Alterman[2] –quien utilizó el término de posverdad para referirse a la presidencia de George W. Bush tras los atentados del 11S–, o Colin Crouch[3] –que acuñó el de *posdemocracia* para destacar cómo la industria publicitaria, ligada a la comunicación política, estaba generando una crisis de confianza en el sistema–.

Para algunos, la posverdad es un concepto fetiche hacia el que profesan cierta veneración por su capacidad para describir la situación actual, derivada de los cambios en el orden internacional surgido tras la II Guerra Mundial. Se puede considerar como

[1] Ralph Keyes, The Post-Truth Era. Dishonesty and Deception in Contemporary Life, St. Martins Press, 2004.

[2] Eric Alterman, When Presidents lie. A History of Official Deception and Its Consequences, Viking, 2005.

[3] Colin Crouch, *Post-Democracy*, Polity Press, 2004.

sinónimo de *mentira emotiva*, esto es, la distorsión deliberada de la realidad con el fin de crear y modelar la opinión pública e influir en las actitudes sociales. Una realidad en la que los hechos objetivos, las referencias fácticas, tienen menos influencia que las apelaciones a las emociones y a las creencias personales.

Esta idea nos conduce a otras, como verdad, mentira, interpretación, opinión, todas surgidas al amparo de las virtudes de la Ilustración, como la duda y la conciencia moral, y explotadas por el relativismo posmoderno, donde no existe una única verdad, sino varios tipos de narración. Esto es lo que Victoria Camps llama "pensamiento débil" y es el que, a su juicio, abre precisamente a puerta a la posverdad.

Ya decía Nietzsche que no existen los hechos, solo las interpretaciones. Hoy las opiniones son sagradas y los hechos, opinables. Justo lo contrario de lo que enseñaban hace algunos años en las facultades de Periodismo, cuya máxima era "los hechos son sagrados y las opiniones, libres". Hoy, al amparo de que la verdad es poliédrica, difícil de definir y de aprehender, se ha minado la confianza en los expertos y en su *expertise* y se ha iniciado una carrera por apropiarse del relato y por ser portador de nuevas verdades.

Matthew d'Ancona[4] está convencido de que vivimos en un mundo de posverdad en el que cada uno elige hoy su propia verdad "como si fuera un *buffet* libre". Un mundo donde se ha erosionado la confianza en las instituciones, donde la globalización ha generado incertidumbres y donde lo digital y las redes sociales han contribuido a reforzar un relativismo pernicioso que se ha ido extendiendo disfrazado de legítimo escepticismo.
En este sentido, la posverdad también nos conduce a la mentira, aunque no son términos equivalentes. Antes quizá muchos lo recuerden, mentir estaba mal visto. Así nos lo enseñaban. La Biblia lo prohibía y Kant decía que la mentira no servía para salvar la vida de un inocente. Pero, en paralelo, Maquiavelo ha ido resucitando hasta el punto de que "la simulación de la verdad aprovecha y la misma virtud estorba". En esta dinámica, la mentira ha dejado de disimularse y, en cierto modo, se ha ido perdiendo la vergüenza.

Como dice Hannah Arendt[5], la mentira siempre ha existido como herramienta necesaria y justificable en la actividad política: "cuando un embustero no puede imponer su mentira dice que es opinión, borrando así la división entre verdad de hecho y opinión". Y, en este ámbito, Arendt señala determinados discursos nacionalistas como punto culminante de la mentira al servicio de la dominación. Discursos donde la mentira, en forma de exaltación de un supuesto interés nacional, viene a avalar un presente inventando un pasado que lo justifique y difundiendo el mito narrativo a través del lenguaje y del sistema educativo. Y a nadie puede escapársele cómo durante el nazismo las élites políticas predefinieron e impusieron su propia comprensión de la realidad a través de la propaganda.

[4] Matthew d'Ancona, Post-Truth. The New war on Truth and How to Fight, Random House, 2017.

[5] Hannah Arendt, *Verdad y mentira en la política*, Página Indómita, 2017.

Tecnología, información y realidad: la burbuja

Cada época ha tenido su tecnología para difundir falsedades y propaganda. Hoy la revolución digital lo ha cambiado todo y se producen más noticias que nunca y se difunden a mayor escala, mundial o local. Noticias que circulan a más velocidad y más eficazmente gracias a una potente infraestructura técnica que hace uso de nuevas prácticas comunicativas que se adaptan con mucha flexibilidad a un comportamiento social cambiante.

Ahora las noticias transitan sin filtro por las redes y las genera más gente. Cada individuo se ha convertido en un medio de comunicación en sí mismo que solo comparte lo que quiere y aquello con lo que está de acuerdo, las más de las veces sin detenerse a pensar. Puede decidir incluso, de manera consciente, aceptar determinadas informaciones para reafirmar sus propias opiniones y aceptar también con ello un lenguaje manipulado, ligado a las emociones, que crea, en consecuencia, una nueva realidad.

Dicen los psicólogos que las emociones negativas se perciben más intensamente que las positivas, y puede que sea así. Sobre este punto, cabe referirse a otra palabra fetiche del mundo digital: *la burbuja de filtros.* La burbuja creada por la tecnología, gran paradoja frente a la globalización, en la que los ciudadanos viven y solo están inmersos y en contacto con ideas u opiniones que coinciden con las suyas. Un mundo donde los algoritmos de Facebook o Google marcan y facilitan el camino de la información, mermando de este modo la capacidad de autocrítica.

La máquina tiende a pensar por nosotros y ha acabado por contagiar nuestra forma de pensar. Las redes sociales han pasado de ser espejo del mundo a convertirse en su directriz. Han pasado de reflejar la vida real a nutrirla con sus modos y sus formas, devolviéndonos nuestra propia realidad jerarquizada, una realidad donde los medios tradicionales, apelando siempre a los hechos, han perdido ese rol de verificadores y, en consecuencia, el papel que les asignábamos para jerarquizar la realidad.

Las redes, además, imponen brevedad. La brevedad del WhatsApp ha desterrado al *email*, que ya aniquiló al fax, y éste, a su vez, a las cartas en papel. Cada vez se escribe menos, con mensajes más cortos que llegan más rápido. La forma ya no es relevante, ni la sintaxis ni el estilo ni, si se me permite, tampoco la ortografía. Importa el mensaje, siempre urgente, que llegue rápido y, a veces, sin escritura, porque para eso están los emoticonos. Pero ¿cuál es la razón de su éxito? La máquina señala el camino: brevedad. Pensemos en Twitter, donde el mensaje va encapsulado en una frase corta, contundente. Brevedad y contundencia, velocidad y eficacia, conceptos que vuelven a situarse por encima de la verdad en la escala de valores.

En este contexto, ¿a quién le importa decir la verdad cuando lo único importante es que lo crean? No importa que se divulguen falsedades completas, lo importante es que parezcan verosímiles. De este modo, la falsedad, lo *fake*, que cuenta con la ubicuidad que le aporta la tecnología, contamina todas las esferas de nuestra vida: la comunicación, la política, la economía, el pensamiento, las decisiones e incluso nuestra vida privada. Y, cuando la falsedad se vuelve más sutil, más compleja, ha sido creada

con una intencionalidad táctica, responde a una estrategia y persigue objetivos, es cuando podemos hablar desinformación.

Desinformación, injerencia y ciberespacio

La desinformación puede definirse como la difusión intencionada de información no rigurosa que busca minar la confianza pública, distorsionar los hechos, transmitir una determinada forma de percibir la realidad y explotar vulnerabilidades con el objetivo de desestabilizar. Y ya no estamos hablando de filosofía; estamos hablando de obtener ventajas políticas, de minar los valores democráticos, de extender una nueva narrativa para, en definitiva, cambiar nuestra realidad. Y también de una forma nueva, barata y eficaz de injerencia, como puso sobre la mesa la posible interferencia rusa en las elecciones estadounidenses de 2016, el referéndum del *Brexit*, los procesos electorales de Francia y Alemania o lo ocurrido en Cataluña.

Aun cuando resulta difícil cuantificar la influencia de una campaña de desinformación, lo que sí resulta evidente es su poder corrosivo a medio y largo plazo. Y, en este sentido, lo que puede resultar más preocupante es, como señala el Atlantic Council[6], que, aunque sea Rusia la que haya desarrollado las técnicas, los actores maliciosos aprenden rápidamente unos de otros y las mismas herramientas creadas por Rusia pueden estar siendo utilizadas por otros actores con el mismo objetivo de debilitar nuestras democracias, un sistema que, por su propia naturaleza, resulta en el corto plazo más vulnerable a la manipulación que los sistemas totalitarios y que, en consecuencia, tiene más dificultades para ofrecer respuestas contundentes, que no pueden ser otras que las que resulten del consenso, que engloben al conjunto de la sociedad, a gobiernos, a medios de comunicación y a la sociedad civil y que confíen en la capacidad de la cooperación internacional con el objetivo de fortalecer nuestra resiliencia democrática.

No obstante, la propia naturaleza cambiante de la desinformación, las dificultades de su identificación como amenaza, su trazabilidad y la determinación de la autoría, unido todo ello a la legítima sensibilidad democrática respecto de eventuales limitaciones de los derechos y libertades fundamentales, obligan a los responsables de la toma de decisiones a extremar la prudencia a la hora de actuar. Además, como señala el Atlantic Council, identificar las soluciones que funcionan y las que no requiere de un método de prueba y error, sin que podamos esperar soluciones definitivas.

De todos modos, como señaló el gobierno francés al presentar a la Asamblea Nacional su proposición de ley relativa a la lucha contra la manipulación de la información: “Ante la impotencia para hacer frente a la producción de noticias falsas, el Estado tiene la responsabilidad de hacer cuanto esté en su mano para limitar su impacto”[7]. Sobre este

[6] Daniel Fried y Alina Polyakova (2018), “Democratic Defense against Disinformation”, Atlantic Council, 5/II/2018, https://www.atlanticcouncil.org/images/publications/Democratic_Defense_Against_Disinformation_FINAL.pdf

[7] Loi n° 2018-1202, du 22 décembre 2018, relative à la lutte contre la manipulation de l'information, http://www.assemblee-nationale.fr/dyn/15/dossiers/fausses_informations_lutte.

punto, cabe recordar que la desinformación se mueve como pez en el agua en el ciberespacio, un lugar que ha dejado de ser la utopía digital con la que soñábamos.
Ya decía Henry Kissinger que el ciberespacio desafiaría toda la experiencia histórica. Y así ha ocurrido. A su juicio, "la definición de lo que hasta ahora constituía la autoridad de los Estados se ha vuelto ambigua y en algunos casos confusa". Durante la Guerra Fría, solo algunos países tenían capacidad de fabricar bombas nucleares. Hoy prácticamente cualquier país o cualquier avezado grupo de *hackers* está en condiciones de lanzar un ciberataque o de propagar determinadas narrativas. Con ello, las fronteras territoriales, antaño definidas y permanentes, hoy aparecen difuminadas. Se difumina también la distinción entre amenazas internas y externas y entre la actividad civil y militar y se alteran las concepciones institucionales en las que vivíamos, lo que nos obliga a crear nuevos procesos de decisión, a reinventar las instituciones o a redefinir las ideas.

Basta pensar cómo están evolucionado conceptos como *transparencia* o *privacidad*, cómo se está diluyendo la separación entre lo público y lo privado y cómo ha variado lo que legítimamente esperábamos de la Administración y lo que ahora es responsabilidad de empresas, organizaciones del sector privado o de los propios ciudadanos. La desinformación puede provenir de Estados, pero también de actores no estatales. Puede tener múltiples y variadas motivaciones. Y, a menudo, su trazabilidad constituye un obstáculo difícil de superar. Además, los objetivos políticos ya no solo se persiguen con herramientas convencionales. La fuerza militar ha cedido terreno en favor de otras más sofisticadas que incorporan todo un abanico de instrumentos (políticos, económicos, económicos y digitales) con la vista puesta en interferir en procesos democráticos, debilitar nuestras instituciones, desestabilizar el tejido social y crear nuevas narrativas.

Ciberespacio, regulación y comunidad internacional

Vivimos en un mundo interconectado: 4.000 millones de personas, más de la mitad de la población del planeta, disponen de acceso a Internet; el 75% de la población mundial tiene acceso a un teléfono móvil y los cuatro grandes (Google, Amazon, Facebook y Apple) reúnen un PIB similar al de Francia. Internet y su hábitat, el ciberespacio, constituyen un bien público global. Y los bienes e intereses públicos globales se gestionan y protegen a través del Derecho Internacional. Para su defensa y protección, las legislaciones nacionales se muestran ineficaces.

Resulta evidente que necesitamos normas, normas *online* como las tenemos *offline.* Malcolm Shaw, que subtitulaba su manual de Derecho Internacional con la frase "En la larga marcha de la Historia desde la cueva hasta el ordenador", destacaba el papel central que juega en nuestra civilización la idea del Derecho[8]. Y, a pesar de que el ciberespacio es común a todos, carece de regulación en el sentido tradicional de la palabra, de una regulación que impida o frene todo aquello a lo que nos enfrentamos. Necesariamente, ello nos remite a Naciones Unidas. La comunidad internacional ha venido trabajando desde hace más de una década mediante cinco "grupos de expertos gubernamentales" (GEG) reunidos bajo el título "Avances en la información y las telecomunicaciones en el contexto de la seguridad internacional".

[8] Malcolm N. Shaw, *International Law*, Cambridge University Press, 2017.

Tan solo los grupos de 2013 y 2015 finalizaron con informes de consenso, que determinaron la aplicabilidad de la Carta de las Naciones Unidas en su totalidad; del Derecho Internacional, incluidos los derechos humanos y el Derecho Humanitario Bélico; la obligación de los Estados de fomentar un ciberespacio abierto, seguro, estable, accesible y pacífico, y el respeto a determinadas normas no vinculantes sobre el comportamiento responsable de los Estados.

Hace unos meses, en la última Asamblea General, parecía que podíamos estar al borde de otro fracaso colectivo, pero el resultado es que estamos ante una situación novedosa que esperamos se desbroce en los próximos meses. Dos serán los foros que abordarán la gobernanza del ciberespacio. Por una parte, un nuevo GEG, impulsado por Estados Unidos y la UE, que partirá de los consensos alcanzados en los grupos anteriores; por otro, un grupo de trabajo abierto (OEWG en sus siglas inglesas), impulsado fundamentalmente por Rusia, que podría buscar la negociación y firma de un tratado internacional en la materia. No obstante, es de prever que tres elementos continuarán dividiendo a la comunidad internacional.

Aunque existe acuerdo sobre la aplicabilidad del art. 7 de la Carta de Naciones Unidas, sobre el principio de no intervención, la aplicación del art. 51, que se refiere al derecho a la legítima defensa en caso de agresión, presenta algunas dificultades que, para salvarlas, tendrían que responder al cómo y al quién, es decir, a atribuir y, al mismo tiempo, a recordar que solo los Estados son sujetos de Derecho Internacional, lo que nos llevaría a su vez a pensar en qué habría de ocurrir si la autoría se sitúa en un actor no estatal, descartando siempre la legítima defensa preventiva, esto es, el actuar por anticipación, lo que no tiene sustento en el Derecho Internacional.

Un segundo elemento de división es el reconocimiento y disfrute *online* de los mismos derechos protegidos *offline*, incluyendo el derecho a la libertad de expresión o el derecho a la privacidad. Y baste recordar que no existe tratado internacional sobre protección de datos, salvo el Convenio 108 del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Y, por último, la concepción misma del ciberespacio, concepciones diferentes que se sustancian en conceptos distintos de soberanía: mientras Occidente apuesta por un ciberespacio libre, abierto, seguro y estable, resultado del esfuerzo conjunto del sector privado, la sociedad civil, la comunidad técnica, los usuarios y la academia, otros se inclinan por la sola y exclusiva presencia de los Estados como actor privilegiado y exclusivo para gobernar la red.

Desinformación y Europa

Y, en este panorama, Europa pretendió avanzar. En 2017 se produjo un salto cualitativo de la mano de la presidencia estonia del Consejo de la UE, un país que sufrió ataques cibernéticos muy relevantes y que hoy es el país digital por excelencia. En ese momento, las perspectivas compartimentadas para hacer frente a la inestabilidad en el ciberespacio dieron paso a un enfoque integral que implicaría a todos los actores e instrumentos disponibles (políticos, diplomáticos, militares y económicos). Se buscó una actitud proactiva, frente a la posición reactiva anterior, que fomentase sinergias para

avanzar hacia una mayor autonomía estratégica (hoy Europa es un importador neto de productos y soluciones de ciberseguridad de proveedores no europeos) y reforzar la cooperación internacional.

Europa reconoció finalmente que la desinformación y, en consecuencia, los riesgos aparejados de interferencia electoral son fenómenos en aumento, de naturaleza transnacional, que afectan de lleno a nuestra seguridad y a la viabilidad de nuestras sociedades libres y democráticas. Y se decidió a abordarla desde dos ámbitos íntimamente conectados: por una parte, reforzando nuestra ciberseguridad (*Cybersecurity Package* entre otras medidas) y, por otra, combatiendo la manipulación de la información y, por ende, de la opinión pública[9].

Para ello se convocó un "grupo de expertos de alto nivel sobre noticias falsas", cuyas conclusiones vinieron a sumarse a las revelaciones ligadas al caso Facebook/Cambridge Analytica (mal uso de los datos personales en contextos electorales), a los resultados del Eurobarómetro (el 83% de los encuestados consideraba la desinformación "un peligro para la democracia"; dos tercios de los consumidores de noticias preferían acceder a ellas a través de las redes sociales o de plataformas algorítmicas) y al hecho de que el poder del mercado y los flujos de ingresos habían pasado de estar en manos de los editores de prensa tradicional a las de los operadores de plataformas, que disponen de datos para concordar lectores, artículos y anuncios[10].

Con todo ello, el presidente Juncker en el discurso sobre el estado de la Unión[11], y con la vista puesta en las próximas elecciones europeas y los más de veinte procesos electorales de diferente naturaleza y procedimiento que tendrán lugar a lo largo de este año en Europa, destacó la necesidad de elecciones "justas, libres y transparentes", reconoció que nunca antes el riesgo de manipulación había sido tan alto y anunció lo que acabaría tomando forma definitiva en el Plan de Acción contra la Desinformación, aprobado en diciembre[12].

Conclusiones

Hemos hablado de retos, de conceptos, de redes sociales. Todo ello para describir un mundo en cambio y en evolución permanente. Un mundo en el que están en discusión muchos de los esquemas establecidos tras la Segunda Guerra Mundial y donde nuestros sistemas democráticos están dejando al descubierto muchas de sus vulnerabilidades.

[9] Comisión Europea, "Reforma de la ciberseguridad en Europa", octubre de 2018, https://www.consilium.europa.eu/es/policies/cyber-security/.

[10] CCN-CERT, "Informe de Buenas Prácticas BP/13: Desinformación en el ciberespacio", febrero de 2019, https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/7680-como-actuar-frente-a-las-campanas-de-desinformacion-en-el-ciberespacio-uno-de-los-mayores-retos-de-seguridad-del-pais.html.

[11] Jean-Claude Juncker, "Discurso sobre el estado de la Unión ante el Parlamento Europeo", 2018, https://ec.europa.eu/commission/priorities/state-union-speeches/state-union-2018_es.

[12] Unión Europea, "Plan de lucha contra la desinformación", diciembre de 2018, https://www.dsn.gob.es/es/actualidad/sala-prensa/uni%C3%B3n-europea-plan-lucha-contra-desinformaci%C3%B3n.

No existen, hoy por hoy, recetas infalibles contra la manipulación de la información. No obstante, resulta evidente que nuestras mejores armas se basan en la convicción, en la capacidad y fortaleza de nuestros propios principios. Y, como señalaba el mencionado Matthew d'Ancona entre sus recetas frente a la posverdad, buscar la verdad en la vida pública es hoy más que nunca una responsabilidad ciudadana.

En consecuencia, no tenemos otra opción más que persistir en la voluntad colectiva e individual de ser capaces de fortalecer nuestra resiliencia democrática y la cooperación nacional, internacional y multilateral. Y, para ello, nada mejor que gobiernos, medios de comunicación, sector privado, sociedad civil y ciudadanía trabajen de la mano.