

## **TECNO- MULTILATERALISMO: LA ONU EN LA ERA DE LA DIPLOMACIA DE LA POSVERDAD**



**Carme  
Colomina**

Investigadora,  
CIDOB

CIDOB REPORT  
# 06- 2020

*Una nueva hibridación del poder mina cada vez más el multilateralismo y afecta al trabajo de la Organización de las Naciones Unidas (ONU). La aceleración tecnológica ha supuesto nuevas interdependencias globales, pero también nuevas vulnerabilidades: la transformación digital de las sociedades y de las economías coexiste con nuevas brechas digitales, la transformación de los paisajes mediáticos, la multiplicación de los actores políticos y comunicativos, y la proliferación de fuentes de información de dudosa trazabilidad, así como erosiones más profundas de la privacidad y los derechos humanos. La esfera digital ha transformado sociedades, políticas, retos y amenazas, pero la maquinaria pesada de la arquitectura de la ONU, regida por equilibrios del pasado y luchas de poder tradicionales, tiene dificultades para adaptarse a esta nueva realidad.*

Imagínese una colección cada vez más amplia de audios y vídeos donde aparezcan líderes globales, como Donald Trump, Vladimir Putin o Xi Jinping, diciendo cosas que no han dicho jamás. Imagínese el impacto político y el descrédito público que tendrían esos discursos falsos, generados con tecnología de aprendizaje automático (AA), en un mundo de incertidumbres, disrupciones políticas y cambios tecnológicos rápidos. Solo se necesitan algunas horas de trabajo, menos de diez dólares (en recursos informáticos en la nube) y acceso a un vasto archivo de discursos de la Asamblea General de las Naciones Unidas para simular un discurso político creíble generado por inteligencia artificial (IA), como ha podido comprobar Global Pulse, la iniciativa de la Secretaría General de la ONU sobre Big Data e IA para el desarrollo, la acción humanitaria y la paz.<sup>1</sup>

1. Véase <https://www.unglobalpulse.org/2019/06/new-study-by-global-pulse-highlights-risks-of-ai-generated-texts-creates-fake-un-speeches/>.

La diplomacia se convierte más que nunca en un campo minado cuando la verdad y la confianza son difíciles de distinguir, cuando ya no podemos creer lo que vemos.

La mentira siempre ha formado parte de la caja de herramientas de la política exterior de los gobiernos. A lo largo de su historia, la ONU se ha visto expuesta a la manipulación estratégica y deliberada, a la desinformación intencionada y a discursos propagandistas. El 5 de febrero de 2003, ante el Consejo de Seguridad de Naciones Unidas, Colin Powell, el que fuera secretario de Estado bajo el mandato del presidente George W. Bush, engañó conscientemente al mundo al acusar al Irak de Saddam Hussein de tenencia de armas de destrucción masiva. Powell (2003) aseguró que solo proporcionaba “hechos y conclusiones basadas en inteligencia sólida” para justificar una guerra que “era ilegal e infringía la carta de la ONU”, según el ex secretario general de la ONU Kofi Annan. ¿Qué ha cambiado desde entonces?

Estamos inmersos en una aceleración tecnológica que ha transformado el concepto de poder, la idea de amenaza y los escenarios de enfrentamiento mundial. El arte de gobernar se ha visto obligado a adaptarse a un paisaje cambiante en que la capacidad militar no es el único poder definitivo, donde los Estados Unidos y la Unión Europea (UE) se sienten desbordados por el desarrollo tecnológico chino, y las nuevas hegemonías de poder se disputan mediante amenazas más difusas e híbridas y en escenarios más diversos. La desinformación tradicional y la de nueva generación tienen más recursos, más capacidad de penetrar en el discurso público y nuevas posibilidades de injerencia política. Todo ello agrava las tensiones sociales e intensifica la polarización pública. Cada vez más, la percepción de los hechos está mediada por las emociones y la idea de lo que es, o no, verdad parece ser una cuestión de libre elección. La transformación de la esfera pública de la que somos testigos no solo se explica por la crisis de los sistemas mediáticos tradicionales, sino por el nuevo orden algorítmico que controla en gran medida la predeterminación selectiva de los contenidos que vemos.

La información lleva implícita un marco mental y unos valores concretos. Así que el espacio informativo está en conflicto no solo por una lucha de poder, sino también por un choque de modelos para determinarlo. Tal como se afirma en el Informe de riesgos globales de 2019 publicado por el Foro Económico Mundial, “las nuevas capacidades tecnológicas han inten-

La información lleva implícita un marco mental y unos valores concretos. Así que el espacio informativo está en conflicto no solo por una lucha de poder, sino también por un choque de modelos para determinarlo. Tal como se afirma en el Informe de riesgos globales de 2019 publicado por el Foro Económico Mundial, “las nuevas capacidades tecnológicas han inten-

sificado las tensiones existentes sobre los valores –por ejemplo, debilitando la privacidad individual o aumentando la polarización–, mientras que son las diferencias en cuanto a valores, precisamente, las que están determinando el camino y la dirección de los avances tecnológicos en diferentes países”. No obstante, la IA también puede ser una herramienta poderosa para el desarrollo internacional. El Banco Mundial, en colaboración con otros socios internacionales como la ONU, está creando el Mecanismo de Acción contra la Hambruna, el cual depende de sistemas de aprendizaje profundo (*deep learning*), desarrollados por Microsoft, Google y Amazon, para detectar crisis alimentarias que se convertirán en hambrunas. UNICEF colabora con el MIT para, a través del aprendizaje automatizado, simular imágenes de grandes urbes internacionales “en ruinas” con el fin de ayudar a empatizar y conectar con el sufrimiento de las personas víctimas de bombardeos, pérdidas y guerras. Hay empresas que usan tecnología de IA en drones autónomos que distribuyen material médico vital, como vacunas, a hospitales rurales de África. Si bien estos ejemplos revelan un potencial enorme para el desarrollo y la ayuda humanitaria, la confluencia de la IA con otras tecnologías emergentes también crea vulnerabilidades sin precedentes y otros riesgos para la seguridad mundial (Pauwels 2019). Mientras arrecia la lucha de poder entre potencias tecnológicas, crecen también las desigualdades cada vez más profundas entre los países usuarios de la tecnología (*tech-taking*) y los países líderes en el desarrollo tecnológico (*tech-leading*). Esta aceleración ensancha la brecha digital y multiplica asimetrías fundamentales.

En este contexto, los pioneros de la digitalización de la diplomacia pública han sido rápidamente derrotados por la nueva realidad. La política a través de las redes sociales ha dejado de estar tan relacionada con la conectividad y la creación de imagen para convertirse más en una herramienta de exhibición pública para alterar las dinámicas políticas tradicionales. La idea de una era de la posverdad no se refiere solo a la capacidad de penetrar en el discurso público con mentiras, sino a una tergiversación real de la verdad cargada sobre todo de intencionalidad. El compromiso diplomático requiere una visión mínimamente compartida y un cierto espíritu de franqueza recíproca para prosperar. Sin embargo, las relaciones internacionales no han podido escapar de esta realidad sesgada por las emociones, en que los hechos son relegados a una posición marginal y la *twiplomacia* ejercida desde los medios sociales

**LA DESINFORMACIÓN  
ENTRAÑA UNA  
AMENAZA A LOS  
DERECHOS HUMANOS  
PORQUE PUEDE  
MINAR EL DERECHO  
A ELECCIONES  
LIBRES Y JUSTAS O  
EL DERECHO A LA NO  
DISCRIMINACIÓN O A  
PROTEGER EL HONOR  
Y LA REPUTACIÓN DE  
UNO MISMO CONTRA  
ATAQUES ILÍCITOS.**

rompe con las dinámicas culturales y los *tempos* tradicionales de la política exterior. En esta era de la posverdad, la información se convierte en un arma arrojadiza para erosionar a la oposición en toda clase de sistemas políticos; líderes todopoderosos de potencias mundiales, en la Casa Blanca o en el Palacio de la Alvorada, pueden difundir mentiras y desinformación desde sus cuentas de Twitter con el fin de avivar la polarización de su propia gente. Tal como señala Laura Rosenberger, “la nueva confrontación entre grandes potencias no tendrá lugar necesariamente en campos de batalla o en salas de juntas; ocurrirá en teléfonos inteligentes, ordenadores y otros dispositivos conectados, y en la infraestructura digital que les da soporte” (Rosenberger 2020). Este escenario de disputa informativa ha generado nuevos dilemas democráticos.

**EL CONCEPTO DE CIBERDELINCUENCIA HA ABIERTO UNA NUEVA PUERTA A LA REPRESIÓN DE DISIDENTES Y DE LA LIBERTAD DE EXPRESIÓN, COMO HAN DENUNCIADO ANTE LA ONU DIFERENTES ORGANIZACIONES DE LA SOCIEDAD CIVIL.**

“En un futuro cercano veremos la emergencia de conflictos cognitivo-emocionales: propaganda a largo plazo impulsada por la tecnología con el fin de generar alteraciones políticas y sociales, influir en las percepciones y propagar el desencanto” (Pauwels, 2019: 16). ¿Cómo puede el multilateralismo imponerse en esta era de diplomacia de la posverdad? ¿Qué clase de gobernanza prevemos para una nueva realidad en la que “los procedimientos automatizados no solo *conocen* nuestro comportamiento, sino que también lo *determinan* hasta el punto de poder modificarlo” (Zuboff 2019: 8)? ¿Qué papel puede desempeñar

la ONU, pendiente desde hace tiempo de reformarse, en esta realidad bipolar dividida entre lo que Shoshana Zuboff acuñó como “capitalismo de vigilancia”, desarrollado por plataformas tecnológicas mundiales contrarias al antiguo sueño digital, y el tecnoautoritarismo de determinados regímenes, reforzado por las incertidumbres de la pandemia de la COVID-19 como excusa para aumentar el control social? ¿Cómo puede el sistema multilateral entender mejor y anticipar los riesgos sin caer en esta bipolaridad?

**La desinformación contra los derechos humanos**

Los derechos de libertad de pensamiento y opinión son fundamentales en cualquier sistema democrático. Así pues, la desinformación entraña una amenaza a los derechos humanos porque puede minar el derecho a elecciones libres y justas o el derecho a la no discriminación o a proteger el honor y la reputación de uno mismo contra ataques ilícitos. Sin embargo, en las posibles respuestas gubernamentales contra esta amenaza, también se ha producido un abuso jurídico y político de lo que se ha clasificado de ma-

nera imprecisa como lucha contra las noticias falsas, pero que en algunos contextos y países ha llevado a la persecución de la libertad de expresión o de los disidentes políticos.

La declaración conjunta de marzo de 2017 del relator especial de la ONU para la Libertad de Opinión y de Expresión, la representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), el relator especial de la OEA para la Libertad de Expresión y la relatora especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), destacó que “el derecho humano a difundir información e ideas no se limita a declaraciones «correctas», este derecho protege también a informaciones e ideas que puedan escandalizar, ofender o perturbar”. Se declararon alarmados “por los casos en que las autoridades públicas han denigrado, intimidado y amenazado a los medios de comunicación, por ejemplo, manifestando que los medios son «la oposición» o «mienten» y tienen una agenda política encubierta” y alertaron de que “las prohibiciones generales de difusión de información basadas en conceptos imprecisos y ambiguos, incluido el criterio de «noticias falsas» («fake news») o «información no objetiva», son incompatibles con los estándares internacionales sobre restricciones a la libertad de expresión [...] y deberían ser derogadas”.

El hecho de que los debates sobre la regulación del ecosistema en línea hayan llegado a la ONU, demuestra los riesgos políticos que entraña la necesidad de fijar estándares comunes para abordar los nuevos retos. Uno de estos debates, sobre el concepto de ciberdelincuencia, ha abierto una nueva puerta a la represión de disidentes y de la libertad de expresión, como han denunciado ante la ONU diferentes organizaciones de la sociedad civil. En diciembre de 2019, las Naciones Unidas adoptaron una resolución encabezada por Rusia y respaldada por China, con el título “lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos”, por 79 votos a favor, 60 en contra y 33 abstenciones, a pesar de la oposición de varias grandes potencias occidentales. La resolución obtuvo los votos favorables de países como Camboya, Corea del Norte, Birmania, Venezuela, Argelia, Siria, Bielorrusia o Kazajistán. Todos los países miembros de la UE, más Canadá, Australia y los Estados Unidos votaron en contra. Los que se oponían al texto temían que la resolución solo sirviera para erosionar la libertad de expresión en línea. Un mes antes de la votación, un grupo de ONG y de asociaciones de derechos humanos mandaron una carta a la Asamblea General de la ONU en la que alertaban de que “la criminalización de actividades habituales en línea por parte de individuos y organizaciones mediante la aplicación de leyes contra la ciberdelincuencia constituye una

tendencia creciente en muchos países del mundo<sup>2</sup> y pusieron en duda la necesidad de una convención específica para esos casos. Pero el choque político que tuvo lugar en la sede de la ONU en diciembre ejemplifica como los diferentes modelos y valores han topado con la realidad digital.

Para la mayoría de países del mundo la preocupación sobre los ciberdelitos tiene menos que ver con ataques de piratas informáticos o usurpación de identidad, y más con la represión de la disidencia política. En consecuencia, la resolución de 2019 criticaba el tratado existente, el Convenio de Budapest sobre ciberdelincuencia, para conseguir que la “lucha contra la ciberdelincuencia” se encamine hacia nuevas vías que faciliten el control informativo y la represión de disidentes políticos. Existe un riesgo real de que el multilateralismo autoritario pueda determinar la gobernanza de Internet.

### **¿Ciberinseguridades?**

La tecnología sigue desempeñando un papel de gran calado en la determinación del panorama de los riesgos mundiales. Los “ataques cibernéticos” y el “fraude y amenaza de datos masivos” se han clasificado durante dos años consecutivos como dos de los principales riesgos mundiales según la lista elaborada por el Foro Económico Mundial (WEF 2019: 152), junto con los enfrentamientos económicos y políticos entre grandes potencias, la erosión de las normas y los acuerdos comerciales multilaterales, la pérdida de confianza en las alianzas de seguridad colectiva, las agendas populistas y nativistas, y las cámaras de resonancia de los medios y las “noticias falsas”. Por lo tanto, es urgente establecer nuevos mecanismos de cooperación en materia de gobernanza de datos. No se trata solo de la carrera actual sobre la propiedad de los datos, sino también sobre el uso que hacemos de estos.

Por eso, esta necesidad de multilateralismo va más allá de los Estados y tiene efectos sobre “nuevos tipos de poder” (Zuboff 2019: 352). La concentración de datos empodera a un número limitado de corporaciones mundiales. Esta proliferación de grandes agentes tecnológicos y la naturaleza interjurisdiccional de la actividad en Internet hacen imposible dar respuesta a los retos del ciberespacio en el ámbito nacional. Sin embargo, “existe una necesidad cada vez más apremiante de establecer directrices, de ámbito nacional e internacional, que acompañen al progresivo y creciente despliegue de la tecnología en contextos civiles y militares” (Pauwels, 2019: 21). Sin embargo, no será fácil hacerlo partiendo de un escenario de dualidad y enfrentamiento estructural. La incoherencia mundial y el conflicto bipolar –personificado en la guerra

2. Véase <https://www.apc.org/es/pubs/carta-abierta-la-asamblea-general-de-naciones-unidas-la-propuesta-de-convencion-internacional>.

comercial y tecnológica entre los Estados Unidos y China, que determina las relaciones internacionales— son la base hasta el momento de las divisiones entre miembros clave de la ONU al intentar establecer algún tipo de regulación.

La seguridad y la estabilidad mundiales dependen cada vez más de la seguridad y la estabilidad digitales, y la ONU también puede ser el espacio para debatir valores y normas sobre este campo, establecer estándares y contribuir al arbitraje y a la resolución de conflictos. Con todo, el reto no es solo cómo asegurar que estos desafíos se abordarán partiendo del multilateralismo, sino también con qué agenda se hará. “Cuando las democracias regulan el contenido y aumentan el control sobre la arquitectura de Internet, debilitan las instituciones democráticas” (Rosenberger 2020). El intercambio abierto y libre de información para empoderar a los ciudadanos a tomar decisiones bien fundadas constituye la base de cualquier sistema democrático. Según las palabras de Laura Rosenberger (2020), “en la filosofía democrática, la información está en manos de los ciudadanos; en la visión autocrática, está en manos de los que ostentan el poder”. Las vulnerabilidades tecnológicas pueden aumentar los déficits democráticos. El reto es cómo establecer un nuevo marco multilateral fuera de la arquitectura del control, que trascienda el conflicto para favorecer la cooperación.

## Referencias bibliográficas

- Bullock, Joseph y Luengo-Oroz, Miguel. *Automated Speech Generation from UN General Assembly Statements: Mapping Risks in AI Generated Texts*. International Conference on Machine Learning AI for Social Good Workshop, Long Beach, United States, 2019. ArXiv:1906.01946
- Organization for Security and Co-operation in Europe. *Joint declaration on freedom of expression and «fake news», disinformation and propaganda*. 3 March 2017 (en línea). [Accedido el 20.08.2020]: <https://www.osce.org/fom/302796>
- Pauwels, Eleonore. *The New Geopolitics of Converging Risks. The UN and Prevention in the Era of AI*. United Nations University Centre for Policy Research, 29 April 2019 (en línea). [Accedido el 20.08.2020]: <https://collections.unu.edu/eserv/UNU:7308/PauwelsAIgeopolitics.pdf>
- Powell, Colin L. *Remarks to the United Nations Security Council*. February 5, 2003, US Department of State Archive (en línea). [Accedido el 20.08.2020]: <https://2001-2009.state.gov/secretary/former/powell/remarks/2003/17300.htm>
- Rosenberger, Laura. *Making Cyberspace Safe for Democracy. The New Landscape of Information Competition*. Foreign Affairs May/June 2020. See <https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy>

Schwarz, Jon. *Lie After Lie: What Colin Powell Knew about Iraq 15 Years ago and What He Told the UN*. *The Intercept*. February 6, 2018 (en línea). [Accedido el 20/08/2020]: <https://theintercept.com/2018/02/06/lie-after-lie-what-colin-powell-knew-about-iraq-fifteen-years-ago-and-what-he-told-the-un/>

United Nations. *The Age of Digital Interdependence*. Report of the Secretary-General's High-level Panel on Digital Cooperation, 10 June 2019 (en línea). [Accedido el 15.08.2020]: <https://digitalcooperation.org/report>

United Nations General Assembly. *Countering the use of information and communications technologies for criminal purposes A/74/401* (25 November 2019), (en línea). [Accedido el 15/08/2020]: <https://www.undocs.org/A/74/401>

World Economic Forum. *The Global Risks Report 2019*. WFE, 15 January 2019, (en línea). [Accedido el 15/08/2020]: <https://www.weforum.org/reports/the-global-risks-report-2019>

Zuboff, Shoshana. *The Age of Surveillance Capitalism. The Fight For a Human Future at the New Frontier of Power*. Londres, Profile Books Ltd, 2019.