DEMOCRACIA Y TECNOLOGÍA DIGITAL

Ted Piccone

• *Los singulares desafíos que la tecnología digital plantea a los gobiernos democráticos y cómo deben responder estos, en colaboración con la sociedad civil* •

RESUMEN

Los gobiernos democráticos se enfrentan a desafíos singulares para maximizar el potencial de la tecnología digital al tiempo que minimizan las amenazas a las sociedades más abiertas. Proteger las elecciones justas, los derechos fundamentales en línea y los enfoques de múltiples partes interesadas respecto a la gobernanza de Internet son tres prioridades interrelacionadas fundamentales para la defensa de democracias fuertes en una era de creciente inseguridad, mayores restricciones y competición geopolítica.

Los crecientes desafíos a los que se enfrentan las democracias para gestionar las complejas dimensiones de la tecnología digital se han convertido en un problema definitorio de la política nacional e internacional con implicaciones directas para los derechos humanos y la salud democrática de las naciones. La digitalización progresiva de casi todas las facetas de la sociedad y la naturaleza inherentemente transfronteriza de Internet plantean una serie de problemas complejos cuando la información pública y privada en línea está sujeta a manipulación, piratería y robo.

Este artículo aborda la tecnología digital en lo que se refiere a tres subtemas distintos pero interrelacionados: elecciones libres y justas, derechos humanos y gobernanza de Internet. En las tres áreas, los gobiernos y el sector privado están luchando para seguir el ritmo de los aspectos positivos y negativos de la rápida difusión de la tecnología digital. Para abordar tales desafíos, los gobiernos y legisladores democráticos, en asociación con la sociedad civil y las empresas de medios y tecnología, deben liderar urgentemente el camino hacia la elaboración e implementación de reglas y mejores prácticas con el fin de proteger los procesos electorales libres y justos frente a la manipulación externa, defender los derechos humanos en línea y proteger la gobernanza de Internet frente a enfoques restrictivos y de mínimos. El artículo concluye estableciendo cuáles deberían ser algunas de esas reglas y mejores prácticas.

PALABRAS CLAVE
Democracia | Internet | Derechos humanos | Ciberseguridad | Elecciones | Gobernanza

1 • Lo que dicen los datos

a - Elecciones libres y justas

Los ataques cibernéticos de gobiernos autoritarios y actores no estatales representan una amenaza clara y creciente para las democracias de todo el mundo debido a su interferencia en elecciones libres y justas. Estos ataques adoptan muchas formas y pueden socavar y desestabilizar los procesos democráticos y la gobernanza de muchas maneras.

Hay al menos cuatro formas en que los ataques cibernéticos pueden influir en las elecciones: 1) manipular hechos y opiniones que informan sobre cómo votan los ciudadanos, por ejemplo mediante cuentas falsas de redes sociales, bots y propaganda; 2) interferir con el acto de votar (por ejemplo, falsificando el registro de votantes); 3) cambiar los resultados de la votación, y 4) socavar la confianza en la integridad del voto.[1] Estas amenazas han procedido de países como Rusia y China y, en los últimos años, se han dirigido a países de todo el Occidente democrático. Por ejemplo, el Servicio General de Inteligencia y Seguridad de los Países Bajos citó específicamente a Rusia, China e Irán como amenazas a la seguridad nacional debido a ciberataques.[2] El Buró Federal de Investigaciones (FBI) y el Departamento de Seguridad Nacional (DHS) de los Estados Unidos publicaron múltiples declaraciones en 2016 que detallaban los vínculos de Rusia con los recientes ataques y filtraciones con la intención de influir en las elecciones estadounidenses.[3] En mayo de 2017, el presidente francés Emmanuel Macron acusó a los medios oficiales rusos de difundir propaganda engañosa y noticias falsas con la intención de influir en los resultados electorales a favor de su oponente.[4]

Ataques similares son cada vez más frecuentes: basta citar el número creciente de ciberataques a empresas públicas y privadas, la interrupción de las comunicaciones por Internet de la Cámara Baja del Parlamento alemán y la difusión de campañas de desinformación y noticias falsas antes del referéndum constitucional italiano y las elecciones presidenciales de Estados Unidos.[5] Los ataques cibernéticos suponen tanto una amenaza directa como indirecta a la integridad del proceso democrático, ya que a menudo están motivados por la intención de socavar el apoyo popular a las democracias, su legitimidad y su autoridad moral.[6]

La manipulación de fuentes de información para el discurso político y la toma de decisiones es particularmente insidiosa y difícil de combatir. Las características distintivas de las formas contemporáneas de propaganda rusa, que pueden presentar contenido polarizado que se hace llegar rápidamente a través de los medios tradicionales y las redes sociales, de manera continua y repetida y con escaso compromiso y consistencia en relación con la realidad objetiva, pueden ser difíciles de contrarrestar para los medios independientes y los gobiernos, y mucho más aún para los ciudadanos.[7] Los actores no estatales de la derecha

radical y la izquierda, y los involucrados en el terrorismo, también están explotando la naturaleza abierta de Internet para múltiples propósitos, en particular para influir en la opinión pública antes y durante las elecciones.[8]

b - Los derechos humanos en línea

Internet puede ser una herramienta que permita tanto proteger como violar los derechos humanos, y que tiene implicaciones directas para la seguridad física y cibernética de las personas. La difusión de la tecnología digital ha ampliado enormemente las oportunidades de los ciudadanos de ejercer su derecho a la libertad de expresión y asociación, participar en la vida cívica y responsabilizar a los funcionarios públicos, todos ellos ingredientes esenciales para la celebración de elecciones libres y justas. Los avances tecnológicos recientes también han contribuido a arrojar luz sobre los abusos contra los derechos humanos cometidos en todo el mundo. Los grupos de víctimas ahora publican, transmiten en vivo y difunden videos y fotografías de abusos en YouTube y otras plataformas, con la esperanza de que en algún momento puedan ser utilizados como prueba en procedimientos de rendición de cuentas. Los investigadores de derechos humanos han utilizado imágenes satelitales para denunciar los abusos en las cárceles políticas de Corea del Norte, la limpieza étnica en Myanmar y posibles fosas comunes en Burundi que de otra manera no podrían haber sido descubiertas.[9]

En los últimos años, sin embargo, también se ha observado un continuo deterioro de los derechos humanos en línea, a pesar de las claras declaraciones de la Asamblea General de las Naciones Unidas y del Consejo de Derechos Humanos respecto al hecho de que los derechos fuera de línea establecidos en el derecho internacional de los derechos humanos también están protegidos en línea.[10] El derecho internacional garantiza los mismos derechos a la privacidad y la seguridad de los datos de una persona en línea que a los archivos que conserve en su hogar. Por ejemplo, la vigilancia masiva de internet, practicada incluso en democracias establecidas, es una violación directa de la seguridad de los datos personales de una persona, como lo es una legislación vaga con una autoridad discrecional significativa para vigilar la vida digital de una persona.[11] Los proveedores de servicios de Internet y las empresas de telecomunicaciones se están quedando atrás de manera drástica en cuanto a ofrecer a los consumidores productos de hardware y software que los protejan adecuadamente de una multitud de ciberataques.[12] El aumento de la disponibilidad de un comercio lícito e ilícito de armas cibernéticas sofisticadas y de herramientas de vigilancia está facilitando ese tipo de ataques, como se ve en los ataques para exigir un rescate de "WannaCry" que unos piratas informáticos llevaron a cabo en 2017 a escala mundial.[13]

La explotación maliciosa de la tecnología también puede afectar a la seguridad física de las personas y los estados. Para empezar, la mayor digitalización de los dos últimos decenios ha creado un "efecto inhibidor" sobre la libertad de expresión, donde los ciudadanos en ciertos países se sienten menos seguros para declarar sus opiniones, sabiendo que sus datos personales son monitoreados o archivados.[14] Mediante el seguimiento de la ubicación, las redes sociales y los cierres de Internet, los problemas de seguridad en

línea también se vuelven físicos, lo que permite a los opositores de la democracia y los derechos humanos amenazar la seguridad física de sus presuntos objetivos.

Los cierres de internet y otras restricciones en relación con la Red por parte de los gobiernos sobre su propia población son algo generalizado, tanto que se han documentado más de 60 cierres en los primeros nueve meses de 2017,[15] justificados por razones de "seguridad nacional" u "orden público".[16] Estos apagones digitales son particularmente peligrosos para los derechos humanos. Por ejemplo, tras el bombardeo del aeropuerto de Estambul y la detención de 11 legisladores prokurdos en 2016, el gobierno turco redujo el acceso a webs de redes sociales y servicios de mensajería como Facebook, WhatsApp y Twitter, con el fin de bloquear la circulación de noticias o fotografías relacionadas con tales hechos.[17] Estos cierres no restablecieron el orden, sino que violaron los derechos básicos y provocaron temor y confusión entre los ciudadanos.

Los cierres de Internet no solo perjudican la gobernanza democrática debido a la supresión de la libertad de expresión y las funciones normales del gobierno, sino que también pueden causar pánico y plantear problemas de salud pública.[18] Asimismo socavan el sistema internacional basado en normas para la gobernanza de Internet y fomentan la competencia estatal para el desarrollo de códigos legales intrusivos y capacidades cibernéticas ofensivas. Por último, es importante señalar que el deterioro de los derechos en línea no es solo una táctica de regímenes autoritarios, sino también de gobiernos democráticos. La falta de mecanismos efectivos de regulación o supervisión del papel de las empresas privadas en la protección de los datos de los ciudadanos es otro elemento del dilema.

A pesar de estas amenazas cibernéticas a los derechos humanos, algunos países se han destacado en la adopción de leyes y códigos de conducta para proteger los derechos en línea de sus ciudadanos. En Brasil, la ley *Marco Civil da Internet* (Marco Civil de Internet) de 2014 "garantiza el derecho a la libre expresión, protege la privacidad de los usuarios, excluye la responsabilidad por contenido web generado por terceros y preserva la neutralidad de Internet".[19] También en 2014, se estableció la Agenda de Tallin para la Libertad en Internet, en la que los miembros de la *Freedom Online Coalition*, entre ellos estados como Canadá, Ghana y los Países Bajos, se comprometieron a promover los derechos humanos en línea y a garantizar la transparencia de sus gobiernos en el uso y protección de datos de los ciudadanos. Sin embargo, el respeto de estos principios, incluso entre Estados signatarios como México y Kenia, es un desafío permanente. El Consejo de Europa aprobó una prometedora Estrategia para la Gobernanza de Internet para 2016-2019, que pone de relieve la construcción de la democracia en línea, la protección de los derechos humanos y la seguridad en línea.[20] Estas leyes, estrategias y coaliciones representan avances prometedores para los derechos humanos y, aunque no carecen de problemas, son pasos en la dirección correcta.

c - Gobernanza de internet

La gobernanza de Internet cumple una función esencial en la protección de los derechos humanos y el mantenimiento de democracias saludables en todo el mundo. Internet se

fundó sobre la base de los principios de la autoorganización descentralizada y el flujo de información transfronteriza, y está dirigida principalmente por actores privados como una red de redes. Sin embargo, la creciente afirmación de la regulación de Internet por parte de los Estados nación y la fragmentación a través de las fronteras jurisdiccionales y territoriales amenazan cada vez más estos principios. Si el acceso a Internet de un país está restringido, eso interfiere con el resto del acceso mundial. Más de 40 gobiernos, entre ellos China y Rusia, han promulgado restricciones sobre la información, los datos y el conocimiento en internet.[21] Según el estudio *Freedom on the Net* 2017 de *Freedom House*, menos del 25% de los usuarios de internet residen en países "libres" donde no hay barreras importantes para el acceso ni restricciones de contenido.[22]

El término "gobernanza de internet" también se refiere a los protocolos internacionales que rigen la interoperabilidad global de internet. El debate en curso sobre los modelos de gobernanza de internet se ha centrado en el deseo de Estados Unidos de continuar el enfoque de múltiples partes interesadas de Internet, en el que los sectores privado, social y gubernamental participan en el modelo de gobernanza.[23] Como ha sido en Estados Unidos donde se ha dado gran parte del crecimiento e innovación de Internet, ese país ha tenido una influencia significativa sobre su organismo rector, la Corporación para la Asignación de Nombres y Números en Internet (ICANN); esto ha llevado a otros países a preguntarse si el enfoque de múltiples partes interesadas está excesivamente sesgado en beneficio del gobierno de los Estados Unidos y del sector privado.[24]

Para abordar estas inquietudes y en el espíritu de preservar una Internet abierta, en septiembre de 2016 el gobierno de Obama decidió no renovar el contrato de Estados Unidos con la ICANN, renunciando así a su influencia predominante y logrando que dicha corporación fuera independiente.[25] Sin embargo, países como Rusia, India y China todavía critican el modelo de múltiples partes interesadas y abogan por un enfoque multilateral centrado en el Estado, que les otorgaría una mayor influencia, ya que serían las instituciones internacionales, como las Naciones Unidas, quienes gobernarían Internet.[26]

Los defensores del enfoque de múltiples partes interesadas, particularmente en los sectores privados y sin fines de lucro, temen que si se promulga un modelo de gobierno multilateral liderado por el Estado, se producirían graves pérdidas en las libertades y la innovación de internet. El enfoque multilateral les da a los países que no comparten los mismos valores democráticos una mayor participación en la gobernanza de internet, lo que permite la introducción más amplia de herramientas antidemocráticas de censura y la soberanía nacional en la Red. China y Rusia ya censuran la internet que pueden controlar dentro de sus fronteras; otorgarles poderes de toma de decisiones en la gobernanza mundial de internet podría llevar a violaciones de los principios fundamentales en los que se fundó la Red.

Brasil introdujo otro enfoque que incorpora principios tanto de múltiples partes interesadas como multilaterales en que se incluyen los componentes privados, sociales y gubernamentales, junto con otros interesados, como el mundo académico y una representación no gubernamental

elegida; ese proceso sería gobernado a su vez por un organismo que les permitiría a los países tener la misma voz en el proceso de toma de decisiones.[27] Aunque este enfoque combina ambos modelos de gobernanza, es poco probable que se adopte sin un amplio apoyo internacional. Como tal, la gobernanza de internet ha ido convirtiéndose cada vez más en un tema en el que las democracias y las autocracias toman lados opuestos, que, según los académicos, es de vital importancia para la seguridad, la apertura y la resiliencia futuras de internet.

2 • Implicaciones y recomendaciones en materia de políticas

A la luz de las amenazas actuales y futuras a la democracia y los derechos humanos que plantean los usos irresponsables y perturbadores de las comunicaciones digitales, ahora es el momento en que los defensores de los derechos humanos han de movilizarse en cuestiones de tecnología digital. Es imprescindible que las acciones gubernamentales no tomen una visión estrecha de la seguridad en la cual la seguridad nacional, el contraterrorismo y la soberanía se sitúen por encima de todo lo demás. Tales estrategias, aunque pueden ser potentes a corto plazo, tienen más probabilidades de contribuir al deterioro de la seguridad global y nacional a largo plazo.

Proteger procesos democráticos. El ambiente para las elecciones libres y justas y la formación de la opinión pública debería hacerse más seguro frente a la influencia extranjera y la piratería. Las propuestas, como en los Estados Unidos, de "señalar el sistema de elecciones como una 'infraestructura crítica', una medida que requeriría reforzar las protecciones de ciberseguridad para las máquinas de votación", sería un buen comienzo.[28]

- Para garantizar la integridad de sus elecciones, las democracias deben actualizar sus sistemas electorales y usar dispositivos que no estén conectados a una red digital,[29] o tener copias de seguridad manuales para los sistemas digitales. La ciberseguridad debe actualizarse continuamente para las tecnologías de votación sensibles relacionadas con las listas de registro de votantes, la votación y la tabulación de resultados.

- Los países deberían considerar la adopción de principios en materia de datos electorales abiertos que permitan a los candidatos electorales y al público verificar la integridad de tales procesos como una garantía adicional y como un medio para establecer la confianza pública en ellos.[30]

- Los gobiernos democráticos deben trabajar con urgencia para detectar y castigar los ataques patrocinados por el Estado y los llamados ataques de piratería "patrióticos" con el fin de detener y evitar la futura interferencia en los sistemas democráticos.[31]

- También deberían desarrollar protocolos para facilitar la cooperación transfronteriza con el fin de sancionar la piratería de la infraestructura electoral y redactar un código de conducta con promesas de no interferencia en las elecciones

de cada uno. También resulta cada vez más urgente proteger el papel de los medios independientes frente a los ataques infundados.

• Las democracias deberían trabajar para generar consenso en foros internacionales acerca de que un ataque cibernético deliberado contra una infraestructura fundamental de los sistemas electorales equivale a un ataque físico en su territorio, viola las leyes internacionales de soberanía y no interferencia en asuntos internos y justifica respuestas de autodefensa.

Proteger los derechos humanos en línea. La comunidad internacional debe aplicar y promover las leyes y mecanismos existentes de derechos humanos y ser implacable en la defensa en línea de los derechos fuera de línea.

• En primer lugar, las democracias deben dar un ejemplo positivo respetando esos derechos.[32] Leyes como el Marco Civil de Internet de Brasil o el nuevo Reglamento General de Protección de Datos de la Unión Europea y las iniciativas de múltiples partes interesadas que privilegian la seguridad y la apertura, como *Freedom Online Coalition*, son ejemplos de leyes e iniciativas concretas que deberían ampliarse y respaldarse.[33]

• Los Estados, en asociación con la sociedad civil y el sector privado, deberían coordinar posiciones para fortalecer las resoluciones y mecanismos de las Naciones Unidas destinados a desarrollar normas adecuadas y un seguimiento, como las resoluciones de la Asamblea General de las Naciones Unidas y el Consejo de Derechos Humanos sobre internet y privacidad impulsadas por Alemania (A/C.3/71/L.39/Rev. 1 de noviembre de 2016) y Brasil (A/HRC/32/13 de julio de 2016).

• Es fundamental que las empresas del sector privado en el ecosistema de Internet establezcan sistemas, productos y protocolos mucho más rigurosos para proteger a los ciudadanos frente a las intrusiones de los Estados y los agentes no estatales.

• Las políticas que rigen las restricciones del contenido en la web y las comunicaciones digitales deben elaborarse cuidadosamente con la participación de todos los interesados pertinentes y de conformidad con el derecho internacional de los derechos humanos, como la libertad de expresión y el derecho a la privacidad y el debido proceso.

Impulsar una gobernanza abierta de Internet. Los países democráticos deberían adoptar una postura más activa y unificada en los debates sobre la gobernanza de internet, ya que el enfoque histórico de *laissez-faire* ya no puede sostenerse.[34] Deben defender que la gobernanza de Internet ha de basarse en los valores de una Internet abierta, diversa, neutral y universal. Debe incorporar cuatro principios clave: 1) liderazgo compartido; 2) libre circulación de información y datos al tiempo que protege la propiedad intelectual y la privacidad individual; 3) enfoques de múltiples partes interesadas con la participación de poderes de Internet tanto emergentes como establecidos y una sociedad civil activa y el sector privado, y 4) enfoques dirigidos por la industria para contrarrestar los ataques cibernéticos.[35]

Establecer un código de gobernanza de Internet. Una coalición de Estados con ideas afines debería establecer un grupo de trabajo sobre ciberseguridad integrado por expertos del gobierno, la industria y la sociedad civil para redactar y proponer un código voluntario de gobernanza de internet. Este código debe reflejar los valores compartidos de fortalecer la gobernanza democrática y la transparencia, la promoción de los derechos humanos, la protección de los datos de los ciudadanos y la defensa del modelo de múltiples partes interesadas.

- Las estrategias que deben tenerse en cuenta al adoptar este código deberían ser la Estrategia para la Gobernanza de Internet 2016-2019 del Consejo de Europa y la Agenda de Tallin para la Libertad de Internet de 2014, así como otros modelos actuales.

- El grupo de trabajo podría ayudar a coordinar la educación especializada y la capacitación para legisladores sobre la compleja relación entre los derechos humanos y la tecnología digital y buscar formas de ayudar a los miembros a desarrollar una mayor capacidad de ciberseguridad para proteger los procesos democráticos.

- Al establecer tales normas, el grupo de trabajo debería considerar las consecuencias para los infractores flagrantes, tal como condicionar la cooperación bilateral al cumplimiento de la ciberseguridad. Deben plantear la siguiente pregunta: ¿cómo deberían responder las democracias a los países que intentan ataques cibernéticos en sus procesos democráticos centrales?

NOTAS

1 • Jakob Bund, *Cybersecurity and Democracy – Hacking, Leaking and Voting* (Paris: European Union Institute for Security Studies, 2016): 3.

2 • Kingdom of the Netherlands, Ministry of the Interior and Kingdom Relations, General Intelligence and Security Service, *Annual Report 2015: A Range of Threats to the Netherlands* (Zoetmeer: General Intelligence and Security Service, 2016).

3 • "GRIZZLY STEPPE - Russian Malicious Cyber Activity," U.S. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI), 2016, visitado el 4 de junio de 2018. Más recientemente, el Comité de Inteligencia del Senado de los Estados Unidos concluyó que los ataques cibernéticos de fuentes gubernamentales rusas lograron acceder a elementos restringidos de la infraestructura electoral. "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," Richard Burr, 8 de mayo de 2018, visitado el 4 de junio de 2018, https://www.burr.senate.gov/imo/media/doc/RussRptInstImt1-%20ElecSec%20Findings,Recs2.pdf.

4 • Michel Rose y Denis Dyomkin, "After Talks, France's Macron Hits out at Russian Media, Putin Denies Hacking." Reuters, 28 de mayo de 2017, visitado el 4 de junio de 2018, https://www.reuters.com/article/us-france-russia-idUSKBN18P030.

5 • Melissa Eddy, "After a Cyberattack, Germany Fears Election Disruption." The New York Times, 8 de diciembre de 2016, visitado el 4 de junio de 2018, https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html; Anne Applebaum, "The Dutch Just Showed the World How Russia Influences Western European Elections." The Washington Post, 8 de abril de 2016, visitado el 4 de junio de 2018, https://www.washingtonpost.com/opinions/russias-influence-in-western-elections/2016/04/08/b427602a-fcf1-11e5-886f-a037dba38301_story.html?utm_term=.79384727c9c9; Jason Horowitz, "Spread of Fake News Provokes Anxiety in Italy." The New York Times, 2 de diciembre de 2016, visitado el 4 de junio de 2018, https://www.nytimes.com/2016/12/02/world/europe/italy-fake-news.html.

6 • Jakob Bund, "Cybersecurity and Democracy - Hacking, leaking and voting." EUISS, noviembre de 2016, visitado el 4 de junio de 2018, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_30_Cyber.pdf; Melissa Eddy, "After a Cyberattack, Germany Fears Election Disruption." The New York Times, 8 de diciembre de 2016, visitado el 4 de junio de 2018, https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html.

7 • Christopher Paul y Miriam Matthews, *The Russian 'Firehose of Falsehood' Propaganda Model* (Arlington: Rand Corporation, 2016): 4, visitado el 4 de junio de 2018, http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.

8 • Alice Marwick y Rebecca Lewis, *Media Manipulation and Disinformation Online* (New York: Data & Society Research Institute, 2017): 19, visitado el 4 de junio de 2018, https://datasociety.net/output/media-manipulation-and-disinfo-online/.

9 • Christoph Koettl, "These Images Don't Lie: Exposing North Korea's Dirty Little Secret." Amnesty International, 5 de diciembre de 2013, visitado el 4 de junio de 2018, http://blog.amnestyusa.org/asia/these-images-dont-lie-exposing-north-koreas-dirty-little-secret/; "Burundi: Satellite Evidence Supports Witness Accounts of Mass Graves," Amnesty International, 28 de enero de 2016, visitado el 4 de junio de 2018, https://www.amnesty.org/en/latest/news/2016/01/burundi-satellite-evidence-supports-witness-accounts-of-mass-graves/; "Burma: 40 Rohingya Villages Burned Since October," Human Rights Watch, 17 de diciembre de 2017, visitado el 4 de junio de 2018, https://www.hrw.org/news/2017/12/17/burma-40-rohingya-villages-burned-october.

10 • David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." Asamblea General de las Naciones Unidas, A/71/373, 6 de septiembre de 2016, visitado el 4 de junio de 2018, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc; "Silencing the Messenger: Communication Apps Under Pressure. Freedom on the Net Report 2016," Freedom House, noviembre de 2016, visitado el 4 de junio de 2018, https://freedomhouse.org/report/freedom-net/freedom-net-2016; Antonio Segura-Serrano, "Internet Regulation and the Role of International Law," *Max Planck Yearbook of United Nations Law* 10 (2006): 191-272.

11 • David Kaye, "Report of the Special Rapporteur," 2016.

12 • Toomas Hendrik Ilves, "A Plan for Making the Cyber World Safe." World Economic Forum, p. 2, 20 de septiembre de 2016, visitado el 4 de junio de 2018, https://www.weforum.org/agenda/2016/09/making-the-cyber-world-safe-will-require-more-collaboration-than-ever-before/.

13 • WannaCry es como se denominó un malware diseñado por hackers de tipo "ransomware" (programa para exigir un rescate) que mantiene los datos de la computadora como rehenes hasta que se paga un rescate. Ian Sherr, "WannaCry Ransomware: Everything You Need to Know." C|net, 19 de mayo de 2017, visitado el 4 de junio de 2018, https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/.

14 • Eileen Donahoe, "Human Rights in the Digital Age." Just Security, p. 1, 23 de diciembre de 2014, visitado el 4 de junio de 2018, https://www.justsecurity.org/18651/human-rights-digital-age/.

15 • Entre ellos se incluyen Bangladesh, Brasil, Burundi, Tayikistán, India, Etiopía, Argelia, Congo, Pakistán, Siria e Iraq. "#KeepItOn," Access Now, 2017, visitado el 4 de junio de 2018, https://www.accessnow.org/keepiton/.

16 • David Kaye, "Report of the Special Rapporteur," 2016; Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year." Center for Technology Innovation at Brookings, octubre de 2016, visitado el 4 de junio de 2018, https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf.

17 • Yasmeen Abutaleb y Can Sezer, "Turkey Appears to Be in Vanguard of 'Throttling' Social Media after Attacks." Reuters, 6 de julio de 2016, visitado el 4 de junio de 2018, http://www.reuters.com/article/us-mideast-crisis-socialmedia-idUSKCN0ZM2O3; Can Sezer and Humeyra Pamuk, "Turkey Blocks Access to Twitter, WhatsApp: Internet Monitoring Group." Reuters, 4 de noviembre de 2016, visitado el 4 de junio de 2018, http://www.reuters.com/article/us-turkey-security-internet-idUSKBN12Z0H4.

18 • "POLICY BRIEF: Internet Governance and the Future of the NetMundial Initiative," Access Now, 2015, visitado el 4 de junio de 2018, https://www.accessnow.org/cms/assets/uploads/archive/docs/POLICYBRIEFInternetGovernanceandtheFutureoftheNetMundialInitiative.pdf; David Kaye, "Report of the Special Rapporteur," 2016.

19 • Carl Meacham, "Is Brazil a Global Leader in Internet Governance?" Center for Strategic and International Studies, 15 de mayo de 2014, visitado el 4 de junio de 2018, https://www.csis.org/analysis/brazil-global-leader-internet-governance. Sin embargo, se necesita más trabajo para fortalecer las leyes de protección de datos de Brasil en consonancia con las nuevas regulaciones adoptadas por la Unión Europea.

20 • "Internet Governance – Council of Europe Strategy 2016-2019," Council of Europe, 2016, visitado el 4 de junio de 2018, https://edoc.coe.int/en/internet/7128-internet-governance-council-of-europe-strategy-2016-2019.html.

21 • John D. Negroponte, Samuel J. Palmisano y Adam Segal, *Defending an Open, Global, Secure, and Resilient Internet* (New York: Council on Foreign Relations, 2013): 13, visitado el 4 de junio de 2018, https://www.cfr.org/report/defending-open-global-secure-and-resilient-internet.

22 • "Manipulating Social Media to Undermine Democracy," Freedom House, 2017, visitado el 4 de junio de 2018, https://freedomhouse.org/report/freedom-net/freedom-net-2017.

23 • Harold Trinkunas e Ian Wallace, "Converging on the Future of Global Internet Governance: The United States and Brazil." Foreign Policy at Brookings, julio de 2015, visitado el 4 de junio de 2018, p. 26, https://www.brookings.edu/research/converging-on-the-future-of-global-internet-governance-the-united-states-and-brazil/.

24 • *Ibid.*

25 • Megan Stifel, "Maintaining U.S. Leadership on Internet Governance." Council on Foreign Relations, 21 de febrero de 2017, visitado el 4 de junio de 2018, https://www.cfr.org/report/maintaining-us-leadership-internet-governance.

26 • Harold Trinkunas e Ian Wallace, "Converging on the Future," 2015, p. 19.

27 • *Ibid.*

28 • Mike Orcutt, "What the DNC Hack Says about Cyber-Based Threats to Democracy." MIT Technology Review, 4 de agosto de 2016, visitado el 4 de junio de 2018, https://www.technologyreview.com/s/602108/what-the-dnc-hack-says-about-cyber-based-threats-to-democracy/.

29 • Sergio Hernandez, "How to Stop Election Cyberthreats." CNN, 5 de noviembre de 2016, visitado el 4 de junio de 2018, http://www.cnn.com/2016/11/05/politics/voting-vulnerabilities-cyberattacks/index.html.

30 • Open Election Data Initiative, Homepage, 2018, visitado el 4 de junio de 2018, http://www.

openelectiondata.net/en/.

31 • Mike Orcutt, "What the DNC Hack Says about Cyber-Based Threats to Democracy," 4 de agosto de 2016.

32 • David Kaye, "Report of the Special Rapporteur," 2016.

33 • *Ibid.*; "POLICY BRIEF," 2015.

34 • Robert K. Knake, "Internet Governance in an Age of Cyber Insecurity." Council on Foreign Relations, 2010, visitado el 4 de junio de 2018, p. 7, https://www.cfr.org/content/publications/attachments/Cybersecurity_CSR56.pdf.

35 • John D. Negroponte et al., "Defending an Open, Global, Secure, and Resilient Internet," 2013; Harold Trinkunas e Ian Wallace, "Converging on the Future," 2015, p. 5.

TED PICCONE – *Estados Unidos*

Ted Piccone es Investigador sénior y ocupa la Cátedra Charles Robinson sobre Política Exterior en la *Brookings Institution*. Ha escrito extensamente sobre los aspectos de política exterior de la democracia y los derechos humanos, en particular en su último libro, *Five Rising Democracies and the Fate of the International Liberal Order*. Este artículo se basa en un informe que redactó para la Comunidad de Democracias en septiembre de 2017 con la inestimable ayuda de Hannah Bagdasar, Carlos Castillo, Jesse Kornbluth y Matthew Koo.

contacto: *TPiccone@brookings.edu*

Recibido en abril de 2018.
Original en inglés. Traducido por Fernando Campos Leza.