Noviembre de 2021
SERIE PODER INCISIVO Y RESILIENCIA DEMOCRÁTICA

Una espada de doble filo

La explotación de las tecnologías emergentes mediante el poder incisivo de China

por Samantha Hoffman

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

FORUM INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

LA SERIE *PODER INCISIVO Y RESILIENCIA DEMOCRÁTICA*

Con el afianzamiento de la integración entre democracias y autocracias generado por la globalización, en sectores fundamentales de las sociedades abiertas se han hecho más aparentes los efectos comprometedores del poder incisivo que afecta la libertad de expresión, neutraliza las instituciones independientes, y desvirtúa el ámbito político. La serie *Poder incisivo y resiliencia democrática* procura realizar un análisis sistemático de los mecanismos utilizados por los regímenes autoritarios para manipular el ecosistema político y censurar la expresión independiente en entornos democráticos, además de poner de relieve las posibles respuestas de la sociedad civil.

Esta iniciativa examina cuestiones que surgen de cuatro ámbitos cruciales relativos a la integridad y al dinamismo de los sistemas democráticos:

- Desafíos a la libertad de expresión y a la integridad del espacio mediático e informativo.
- Amenazas a la indagación intelectual.
- Impugnación de los principios rectores de la tecnología.
- Aprovechamiento del capital del Estado con fines políticos y usualmente corrosivos.

El actual resurgimiento del autoritarismo se suscita en el marco de una prolongada regresión democrática mundial que ha deteriorado la confianza de las democracias. Los principales actores autoritarios ponen a prueba a la democracia en el plano de las ideas, de los principios y de los estándares, aunque solamente una de las partes parece estar compitiendo seriamente en la contienda.

La interdependencia del mundo ha presentado complicaciones diferentes de las de la época de la Guerra Fría, en la que los regímenes autoritarios no contaban con tantas oportunidades de acción en el seno de las democracias. En el ámbito interno, Beijín, Moscú y otros regímenes han utilizado instrumentos y tácticas del siglo XXI para afianzar la censura y manipular a los medios y a otras instituciones independientes. Más allá de sus fronteras recurren a emprendimientos educativos y culturales, medios de comunicación, laboratorios de ideas, iniciativas en el sector privado, así como a otros canales de participación destinados a ejercer su influencia en la esfera pública para conseguir sus propios fines, al tiempo que perfeccionan sus técnicas. Cada vez más dichas acciones moldean la indagación intelectual y la integridad del espacio mediático, además de afectar las tecnologías emergentes y la formulación de normas. Entretanto los autócratas recurren a sus sistemas de capitalismo de estado, mayormente híbridos, a fin de insertarse en los mercados y en las economías de las democracias en formas que antes resultaban prácticamente inconcebibles.

El nuevo entorno exige ir más allá de los instrumentos necesarios (aunque insuficientes) de la legislación, la normativa y las demás soluciones gubernamentales. Las democracias cuentan con una ventaja esencial que no poseen los sistemas autoritarios: la creatividad y la solidaridad de sociedades vibrantes que pueden coadyuvar a la protección de las instituciones y fortalecer los valores democráticos. Es así que los trabajos de esta serie procuran contextualizar la naturaleza del poder incisivo, catalogar las principales medidas y esferas autoritarias, y proporcionar ideas para la consecución de acciones no gubernamentales esenciales para la consolidación de la resiliencia democrática.

LA AUTORA

La Dra. Samantha Hoffman es analista principal del Centro Internacional de Políticas Cibernéticas (*International Cyber Policy Centre*) del Instituto Australiano de Políticas Estratégicas (*Australian Strategic Policy Institute*). En 2018 fue investigadora visitante en el Instituto Mercator de Estudios sobre China (*Mercator Institute for China Studies*), sito en Berlín. Se desempeñó asimismo como consultora del Instituto Internacional de Estudios Estratégicos (*International Institute for Strategic Studies*) y de IHS Markit. En sus investigaciones explora las implicancias nacionales y mundiales de la metodología de seguridad estatal aplicada por el Partido Comunista de China, además de presentar nuevas perspectivas para entender y dar respuesta a las acciones chinas de control social y político potenciadas por la tecnología. La Dra. Hoffman cuenta con un doctorado en política y relaciones internacionales de la Universidad de Nottingham (2017), una maestría en estudios chinos modernos de la Universidad de Oxford (2011) y títulos universitarios en asuntos internacionales y lenguas y culturas de Asia Oriental de la Universidad Estatal de Florida (2010). Ha sido autora de artículos para las publicaciones *Foreign Policy, The Hill, War on the Rocks, National Interest, China Brief, Forbes,* y *Jane's Intelligence Review.* Medios tales como el *New York Times, Economist*, BBC, ABC (Australia), *Foreign Policy, Wall Street Journal, Washington Post, Financial Times, Science Magazine,* y *WIRED*, entre otros, la citan ampliamente en lo referente a cuestiones de política y seguridad estatal de China.

AGRADECIMIENTOS

El *International Forum for Democratic Studies* (Foro Internacional de Estudios Democráticos) desea agradecer a Kara Frederick y a Dahlia Peterson por su valiosa revisión por homólogos, y adicionalmente a Shanthi Kalathil, Peter Mattis, Daniel O'Maley, David Shullman, Jack Herndon, Nathan Atrill, y Fergus Ryan por sus comentarios. El Foro desea reconocer a Tyler Roylance por su excelente apoyo editorial y a Daniel Giglio por su excepcional traducción. Agradece asimismo los aportes de Christopher Walker, Jessica Ludwig, Kevin Sheives, John Engelken, y de los demás colaboradores de la *National Endowment for Democracy* (Fundación Nacional para la Democracia). Nuestro agradecimiento a la Fundación Smith Richardson por el esencial apoyo financiero que proporcionó a esta iniciativa.

Las opiniones que se expresan en el presente trabajo representan los puntos de vista y el análisis de la autora y no necesariamente reflejan los de la National Endowment for Democracy ni los de su personal.

Este reporte es una traducción de "Double-Edged Sword: China's Sharp Power Exploitation of Emerging Technologies," originalmente publicado en abril de 2021.

RESUMEN EJECUTIVO

Las tecnologías emergentes ofrecen numerosas comodidades y capacidades que benefician a consumidores y a gobiernos por igual, aunque implican riesgos inherentes que pueden presentar amenazas para las democracias liberales cuando se ven potenciadas por poderosas dictaduras que procuran intensificar y difundir su autoritarismo.

La República Popular China (RPC) potencia las tecnologías emergentes a fin de socavar la estabilidad y legitimidad de las democracias y ampliar su propia influencia. Beijín ejerce un "poder incisivo" que le permite restringir el acceso a la información, distorsionar los entornos políticos y emprender acciones de censura y vigilancia. En este nuevo contexto resulta importante considerar los mecanismos utilizados por Beijín para hacer uso de las tecnologías emergentes como una espada de doble filo destinada a proteger y a expandir su propio poder al moldear, manejar y controlar sus entornos nacionales y mundiales.

La RPC ha desarrollado la tecnología de las "ciudades inteligentes," la cual ha exportado a todo el mundo, lo cual revela la naturaleza del poder incisivo y del autoritarismo potenciados tecnológicamente. El Partido Comunista de China (PCC) recurre a dichas tecnologías para vigilar a su pueblo y controlar a la sociedad. No realiza una distinción clara entre los bienes públicos básicos, como la seguridad vial o la prevención de los delitos violentos, y la represión autoritaria del pluralismo y del disenso. El PCC fusiona esos dos elementos y da prioridad a la seguridad del régimen por sobre los derechos esenciales. En todo el mundo los gobiernos suelen estar deseosos de adoptar las tecnologías de las ciudades inteligentes, por lo que las implicancias de recurrir a sistemas de vigilancia con sede en la RPC y aplicables internacionalmente resultan graves.

Beijín tiene un papel activo en el establecimiento de normas internacionales aplicables a las tecnologías emergentes. La participación en el desarrollo y diseño de dichas tecnologías permite que la RPC las explote a fin de potenciar sus competencias de poder incisivo. El plan denominado Normas de China 2035 prevé la exportación al mundo de las normas de la RPC relativas a tecnologías emergentes y la aceptación de las normas chinas a través de los órganos de normalización. De producirse la aceptación internacional de las normas técnicas originadas en la RPC los sistemas elaborados en China gozarán de una mayor interoperabilidad y acceso al mercado en el resto del mundo, con las correspondientes implicancias para la integridad democrática.

A fin de combatir el poder incisivo en el ámbito tecnológico es preciso que la sociedad civil considere las acciones que se indican a continuación.

- **Fomento del discurso público en materia de tecnología y valores democráticos liberales** para lograr una mejor comprensión de las amenazas del poder incisivo, incluso por medio de programas de alfabetización digital. Es preciso capacitar a las organizaciones de la sociedad civil en temas relativos a las tecnologías emergentes para que puedan ofrecer programas educativos sobre las mejores prácticas en la seguridad de los datos. Por ejemplo, podrían diseñarse programas de alfabetización digital que vayan más allá de los métodos básicos personales y empresariales de gestión de datos e incluyan un análisis de la dimensión geopolítica de los asuntos así como de los mecanismos de abuso de las acciones de recolección de datos aparentemente inocuas.

- **Los grupos de la sociedad civil deben participar activamente en los organismos internacionales de normalización,** tales como la UIT, la ISO y la CEI a fin de contribuir a la elaboración de normas rectoras de las tecnologías de 5G y de internet de las cosas, entre otras, y de contrarrestar las acciones lesivas de la RPC dirigidas a ese mismo propósito. Las organizaciones de la sociedad civil pueden ejercer presión para lograr transparencia en la elaboración de normas técnicas aplicables a las tecnologías que puedan afectar negativamente las libertades civiles, como en el caso de los sistemas de reconocimiento facial o de voz.

- **Las organizaciones mediáticas y de la sociedad civil deben colaborar en forma coordinada a fin de exponer y difundir ampliamente en sus países los indicadores del poder incisivo potenciado por la tecnología,** lo que contribuiría a una mayor concientización pública de las cuestiones, incentivaría el debate de las medidas necesarias, y presionaría a los gobiernos para que tomen medidas de protección.

Las tecnologías emergentes reconfiguran las interacciones del ser humano con su entorno, los métodos empresariales de provisión de servicios, y los mecanismos gubernamentales para la resolución de problemas. Estas tecnologías, que incluyen los instrumentos de "inteligencia de datos," los sistemas integrados de gestión urbana conocidos como ciudades inteligentes, así como lo que se ha dado en llamar el internet de las cosas, ofrecen varias comodidades y capacidades prácticas, a la vez que presentan riesgos inherentes. El peligro surge no solamente de la intención del actor que introduce la tecnología, ni de su propósito original, sino también del propósito de cualquiera de los actores que logre acceder a los datos generados por dicha tecnología. Siempre existe la posibilidad de que esa información se utilice con fines que vayan más allá de los establecidos al momento en la que se la recabó inicialmente: la amenaza aumenta únicamente ante la ausencia de un control democrático.[1] La implicación de los gobiernos autoritarios, con sus intereses particulares y sus criterios jurídicos o normativos, abre la posibilidad de que las tecnologías emergentes socaven gravemente la práctica democrática.

Si bien los regímenes autoritarios comparten ciertas características clave, sus respectivas metodologías de acción y objetivos declarados varían considerablemente.[2] En lugar de procurar una descripción de todos ellos el presente trabajo se centra en la República Popular China (RPC) a efectos de explicar el pleno alcance de los riesgos de las tecnologías emergentes para las democracias liberales cuando dichas tecnologías se hallan impulsadas por un régimen poderoso cuyo objetivo expreso es transformar al mundo para dar cabida a su autoritarismo.[3] Aunque las implicancias del auge tecnológico chino en materia de seguridad nacional se encuentran bien documentadas[4] y los gobiernos democráticos han comenzado a tomar medidas para abordarlo, aún no se ha examinado integralmente la amenaza que implica para las normas e instituciones democráticas. La RPC ocupa necesariamente un primer plano en el debate internacional sobre los riesgos políticos relativos a las tecnologías emergentes, dado que aloja a muchas empresas líderes que exportan su producción a todo el mundo. Si bien varias de esas empresas con sede en China son nominalmente privadas, su derecho de operar en la RPC, así como su éxito, dependen en última instancia de su disposición y capacidad para servir a los intereses del Partido Comunista de China (PCC).[5]

El PCC utiliza la tecnología para ampliar su poder e influencia: la frase *autoritarismo potenciado por la tecnología* constituye la mejor forma de describir esa situación. En lugar de crear mecanismos fundamentalmente nuevos para controlar a las poblaciones, la tecnología amplía los métodos a los que recurre el partido desde hace ya mucho tiempo para ejercer su dominancia autoritaria. A la fecha las repercusiones internacionales del autoritarismo potenciado por la tecnología que aplica el PCC se hallan enormemente subestimadas. Los analistas suelen centrarse en las medidas de coerción y de vigilancia inherentemente invasiva en lugar de tener en cuenta de que los mecanismos tecnológicos que coadyuvan a la resolución de problemas cotidianos y a la prestación de servicios públicos pueden al mismo tiempo incrementar el poder autoritario.

Los enfoques demasiado estrechos en materia de evaluación de riesgos han favorecido un debate público igualmente restringido entre las democracias liberales y en el seno de éstas. A título ilustrativo puede mencionarse que las conversaciones relativas a prohibir que el gigante de telecomunicaciones chino Huawei construyera redes móviles de quinta generación (5G) se han centrado en que las empresas de ese tipo constituyen posibles instrumentos de espionaje de la RPC. No obstante, la recopilación masiva de datos que realizan las sociedades como Huawei en el curso normal de sus actividades puede facilitar varias otras prácticas que perjudican los intereses de las democracias liberales. Por ejemplo, la intensificación en la recolección de datos de alta calidad puede mejorar la precisión de los sistemas de reconocimiento facial y de voz, de análisis de sentimientos, o de diagramas de relaciones. Si bien los gobiernos autoritarios no son los únicos que procuran el desarrollo de estas capacidades, la probabilidad de que el sistema regulatorio de una democracia liberal logre controlar eficazmente la recolección y uso de los datos se ve considerablemente disminuida cuando la empresa en cuestión tiene su sede en un estado autoritario.

En un contexto geopolítico estos riesgos se intensifican ya que algunas autocracias procuran potenciar la tecnología para sus acciones más amplias dirigidas a socavar la estabilidad y legitimidad de las democracias, y a expandir sus respectivas influencias en el mundo. La tecnología contribuye directa e indirectamente a la proyección del poder autoritario, el cual claramente no es ni "blando" ni "duro": su denominación más precisa es "poder incisivo" (sharp power). Según Christopher Walker y Jessica Ludwig el poder incisivo "no se refiere primordialmente a la atracción o a la persuasión, sino que se centra en la distracción y en la manipulación." A diferencia del poder blando, el incisivo "atraviesa, penetra o perfora los ámbitos informativos y políticos de los países a los que se dirige."[6] Procura además "limitar la libre expresión y distorsionar los entornos políticos."[7] La tecnología puede ser una herramienta directa de poder incisivo cuando se la utiliza para la censura o la vigilancia o como plataforma de operaciones de información. De forma más indirecta la tecnología intensifica la capacidad de los regímenes autoritarios de comprender a los públicos que desean influenciar o de proyectar el poder incisivo y mejorar de ese modo otras metodologías para hacerlo. Para entender las ramificaciones de esa situación es importante considerar los mecanismos que utiliza Beijín para recabar tecnologías emergentes con el propósito de proteger y expandir su propio poder mediante el moldeado, el manejo y el control de sus entornos operativos nacionales e internacionales.

EL AUTORITARISMO CHINO POTENCIADO POR LA TECNOLOGÍA: TECNOLOGÍAS DE LAS CIUDADES INTELIGENTES

El desarrollo de las ciudades inteligentes efectuado por la RPC a nivel nacional junto con su exportación al mundo de los correspondientes productos y servicios elaborados por empresas chinas muestran dan una imagen práctica del autoritarismo potenciado por la tecnología. La figura de la "gestión social" (o de la "gobernanza social") constituye la mejor forma de comprender este fenómeno. El concepto hace referencia a los intentos de la dirigencia de moldear, manejar, y controlar a la sociedad, así como a los propios miembros del partido, por medio de mecanismos de cooperación y de coerción. Cabe notar que ese mismo concepto aparece en el sistema de gobernanza mundial del PCC. En el marco del liderazgo partidario de Xi Jinping se ha utilizado la expresión "gestión social internacional" para describir los métodos que emplea el régimen para procurar un nivel similar de control de su ámbito operativo extranjero.[8]

Las ciudades inteligentes implican el uso de tecnologías digitales tales como "los sensores del internet de las cosas, las videocámaras, los medios sociales, y demás insumos que actúan como un sistema nervioso y brindan información constante a los ciudadanos y al operador de la ciudad a fin de que puedan tomar decisiones fundamentadas."[9] La idea de las ciudades inteligentes, independientemente del lugar geográfico en el que se encuentren, es potenciar las tecnologías existentes y emergentes para mejorar la eficiencia y la calidad de los servicios urbanos. Además de los dispositivos para la recolección de datos y las cámaras de vigilancia, las tecnologías de las ciudades inteligentes incluyen plataformas de visualización de datos y de almacenaje en la nube, así como instrumentos de procesamiento de información en tiempo real.

Es posible que la capacidad de las tecnologías de las ciudades inteligentes de mejorar y agilizar la prestación de servicios se vea opacada por su carácter invasivo y de fomento del control político, y susciten la

Es posible que la capacidad de las tecnologías de las ciudades inteligentes de mejorar y agilizar la prestación de servicios se vea opacada por su carácter invasivo y de fomento del control político, y susciten la cooperación de usuarios que se hallan concentrados en los beneficios inmediatos y tangibles en lugar de en las desventajas (generalmente) menos inmediatas.

cooperación de usuarios que se hallan concentrados en los beneficios inmediatos y tangibles en lugar de en las desventajas (generalmente) menos inmediatas. En China las ciudades inteligentes son el último elemento de una larga serie de acciones de gobierno electrónico que datan de principios de la década de 1990, cuando se lanzaron los denominados "proyectos dorados" dirigidos a "construir y modernizar los sistemas de información y a conectar a los organismos a fin de mejorar su capacidad operativa."[10] Estas y otras iniciativas, como las de "gestión de la red," se centraron en la mejora de la seguridad pública y de la gobernanza cotidiana mediante el aumento de la eficiencia burocrática y la resolución anticipada de problemas. En términos generales todas se encontraban vinculadas al concepto de gestión social del PCC.[11] Las ciudades inteligentes de la actualidad también se encuentran asociadas a dos proyectos relacionados y en marcha en materia de seguridad pública: Skynet, lanzado en 2005, y Ojos Atentos (*Xueliang*), iniciado en 2015.[12] Skynet hace referencia al equipo de vigilancia por videocámara que mayormente se encuentra en las principales intersecciones viales, puestos de control policíaco, y demás sitios públicos. Utiliza diagramas cartográficos del Sistema de Información Geográfica (SIG), recopilación de imágenes y mecanismos de transmisión, así como otras tecnologías dedicadas a mejorar la vigilancia y el registro de información en tiempo real.[13] Ojos Atentos es una versión más avanzada de Skynet que se basa en la infraestructura de este último[14] y se centra en la instalación de plataformas de compartición de información de imágenes de video y en el establecimiento de centros de gestión integral en zonas rurales. Ojos Atentos proporciona información de trabajo en materia de seguridad de estado, antiterrorismo, logística mejorada, supervisión de seguridad y prevención, y control de actividades delictivas.[15]

El PCC piensa que es posible que el suministro diario de bienes públicos básicos como la seguridad vial o la prevención de delitos violentos, por un lado, y la proyección del poder autoritario, incluida la supresión del disenso, por el otro, operen de manera conjunta. Los conceptos como el de gestión social fusionan los dos elementos, a la vez que hacen que la seguridad del sistema prevalezca por sobre los derechos y la seguridad del público.[16] Por ejemplo, un medidor inteligente de corriente eléctrica puede mejorar la precisión, transparencia, y confiabilidad de las lecturas, lo que redunda en beneficio de la empresa de electricidad y de sus clientes.[17] En lo relativo a las fuerzas policíacas, es posible que los datos de ese mismo medidor puedan facilitar la detección de conductas "anormales" que podrían ser indicadoras de reuniones "ilegales." Cabe notar que las tecnologías de las ciudades inteligentes se hallan desplegadas de modo más coercitivo en las regiones autónomas de Xinjiang y Tíbet, en donde la población de etnia tibetana y uigur es víctima de graves violaciones a los derechos humanos. En investigaciones realizadas por Human Rights Watch se han descrito los mecanismos utilizados por las autoridades para elaborar una Plataforma Integrada de Operaciones Conjuntas a fin de recabar información sobre conductas individuales y poner de relieve "las que se consideren como posibles amenazas."[18]

El PCC piensa que es posible que el suministro diario de bienes públicos básicos como la seguridad vial o la prevención de delitos violentos, por un lado, y la proyección del poder autoritario, incluida la supresión del disenso, por el otro, operen de manera conjunta.

Resulta fácil que estos abusos nos hagan olvidar que los proyectos de ciudades inteligentes surgieron mucho antes en otras regiones del país con un formato evidentemente menos coercitivo.[19] Además de los aspectos de vigilancia, las tecnologías de las ciudades inteligentes se conciben para la creación de un gobierno más "orientado al servicio." Ese aspecto exige una mejor coordinación intragubernamental de criterios técnicos y de políticas, así como una mejora del funcionamiento del gobierno en general.[20] Al igual que otros gobiernos el régimen del PCC debe resolver problemas corrientes. Los equipos de las ciudades inteligentes contribuyen a la consecución de esa labor. Los sistemas del tipo "cerebro de la ciudad," por ejemplo, integran datos de los órganos gubernamentales a fin de mejorar la gestión del tráfico.[21] Los sistemas de transporte inteligente procuran una combinación de las tecnologías de la información, navegación y posicionamiento, así como las telecomunicaciones y demás capacidades, a fin de

mejorar las redes de transporte.[22] Los sistemas del tipo "cerebro de las ciudades" que supervisan los flujos del tráfico pueden incluso utilizarse para mejorar los tiempos de respuesta de la policía, de los paramédicos, o de los bomberos. Asimismo, los servicios de geocercas (fronteras virtuales alrededor de localidades físicas) pueden servir para todo, desde publicidades focalizadas hasta el rastreo de los movimientos de una persona o vehículo.[23] Puede potenciarse la misma tecnología para facilitar la gestión de desastres naturales, crisis de salud pública o situaciones de graves disturbios civiles.

Los gobiernos de los países en desarrollo suelen demostrar un particular entusiasmo por la adopción de soluciones similares en materia de ciudades inteligentes como mecanismos de modernización de la gobernanza y de mejora de la seguridad. Con el propósito de favorecer el desarrollo de proyectos de ciudades inteligentes en África, en 2018 Huawei informó haber establecido un fondo de 1500 millones de dólares a efectos de "mejorar el tráfico y la calidad del aire de las ciudades, así como la gestión de otros flujos (incluidos los correspondientes a aguas y desechos), promover la eficiencia energética edilicia y contar con servicios inteligentes en materia sanitaria y de atención a la salud."[24] En algunas localidades los proyectos de Huawei han sido vinculados explícitamente con la vigilancia y la seguridad política. Según un informe de 2019 del *Wall Street Journal*, Huawei contribuyó a la construcción de once centros de supervisión de la seguridad pública en Uganda; se determinó además que los técnicos de la empresa prestaron su colaboración cuando los agentes de inteligencia ugandeses solicitaron acciones de vigilancia dirigidas a prominentes políticos de la oposición.[25] Existen otros sistemas inteligentes que se hallan más expresamente asociados con la prestación de servicios. A mediados de 2020 los medios chinos informaron que en Egipto Huawei había sostenido conversaciones con el Ministerio de la Electricidad a fin de transformar el sistema eléctrico del país en una red inteligente con el propósito de optimizar la gestión energética.[26] De igual modo, en 2017 el Ministerio de Comunicaciones de Nigeria indicó que se asociaría con Huawei para el desarrollo de ciudades inteligentes con el objeto de "promover los datos abiertos y favorecer la gestión de los recursos públicos, lo cual a la vez facilita la mayor obtención de ingresos para el gobierno."[27] Independientemente de la intención o finalidad originales, todas estas tecnologías podrían utilizarse con propósitos coercitivos, como sucede en la RPC, si no se las somete a un control democrático efectivo.

Los datos pueden favorecer el uso coercitivo de la tecnología en otros entornos, independientemente del lugar en el que se los haya recabado. El análisis de datos y la inteligencia artificial dependen de grandes cantidades de datos de alta calidad.[28] A título ilustrativo puede señalarse que la tecnología de reconocimiento facial resulta más precisa cuando se la entrena con una mayor cantidad y diversidad de imágenes de rostros. En 2018 el gobierno de Zimbabue celebró un acuerdo con la empresa china CloudWalk para la elaboración de un sistema de vigilancia y una base de datos de reconocimiento facial a nivel nacional.[29] En dicho acuerdo Zimbabue aceptó remitir datos biométricos de sus ciudadanos a la RPC a fin de mejorar la capacidad del sistema CloudWalk para reconocer caras de distintos grupos étnicos y raciales, lo cual le daría a la empresa un mayor nivel de competitividad internacional.

Las implicancias de los mencionados sistemas de inteligencia artificial de aplicación mundial con sede en la RPC son graves, especialmente si las autoridades chinas colaboran con las fuerzas del orden de otros países. Huawei ha indicado que su proyecto en Serbia fue "inspirado" por un incidente en 2015 en el que el sospechoso en un accidente vehicular en Belgrado se fugó a China, en donde fue identificado y detenido en un plazo de tres días gracias a la tecnología avanzada de reconocimiento facial de la RPC.[30] Dada la práctica de acoso del PCC a exiliados y a disidentes que se encuentran en el exterior, y su inobservancia de la ciudadanía legal de nacionales de otros países nacidos en China o de etnia china,[31] resulta claro que podrían explotarse en otros contextos alianzas similares con fuerzas del orden, sumadas a la ayuda brindada por los sistemas de vigilancia inteligente. Por ejemplo, Huawei suscribió varios convenios con Turkcell, el operador líder de servicios móviles turco, entre los que se encuentra un acuerdo de cooperación para la gestión urbana mediante ciudades inteligentes.[32] Existe ya una considerable cooperación entre

Turquía y China con las fuerzas del orden:[33] los nuevos vínculos técnicos podrían implicar aún más peligros para la gran población de uigures exiliados en Turquía.[34] Se han documentado muchos casos en los que las autoridades turcas han facilitado la repatriación forzada de uigures a la RPC.[35]

Incluso cuando estas tecnologías se exportan a municipalidades ubicadas en democracias liberales establecidas, como la de Valenciennes en el norte de Francia o la de Duisburg en Alemania[36] en donde el riesgo de mal uso intencional es menor, la aceptación de sistemas diseñados para su uso en estados autoritarios aún genera varios problemas. La adopción de estas tecnologías en las democracias liberales podría contribuir a la normalización de su utilización en países con salvaguardas jurídicas y regulatorias más débiles. Asimismo, los productos podrían habilitar restricciones directas a la libertad de expresión establecidas por el PCC respecto de personas que en otras circunstancias podrían estar protegidas por las instituciones democráticas. Por ejemplo, la Ley de Seguridad Nacional de 2020 que el gobierno central de Beijín le impuso a Hong Kong tipifica como delito los actos de separatismo, subversión, terrorismo, y colusión con potencias extranjeras aun si el sospechoso se ubica en el extranjero.[37] En el marco de la mencionada ley los hongkoneses, nacionales chinos y otros individuos que cursan en universidades extranjeras podrían ser responsabilizados penalmente por sus declaraciones sobre temas relacionados, en especial si se ven obligados a realizar sus estudios en el territorio de la RPC debido a las restricciones a los viajes causadas por la pandemia de COVID-19. Se informa que en el Reino Unido algunas universidades tienen un proyecto piloto con una herramienta didáctica en línea de Alibaba Cloud que cumple las normas legales y regulatorias de la RPC en materia de contenido y de moderación del contenido.[38] Aun si se interrumpiera ese proyecto específico es preciso que las universidades de los países democráticos hallen alguna forma de hacer frente a la legislación de la RPC para comunicarse con sus alumnos que se encuentren en territorio chino durante la pandemia.

INSEGURIDAD DEL RÉGIMEN: COMPRENDER LA MOTIVACIÓN DE LAS INICIATIVAS TECNÓLOGICAS DEL PCC

Esencialmente la seguridad estatal de la RPC es en realidad la seguridad del partido, independientemente de las fronteras del Estado, en especial en lo relativo a los ámbitos ideológico y político.

Para apreciar el desafío que impone la tecnología como instrumento de proyección del poder incisivo es preciso que los gobiernos democráticos reconozcan que los diversos actores tienen diferentes intenciones. La estrategia del PCC no es un reflejo de las operaciones de desinformación rusas ni de las estrategias de otros regímenes autoritarios, incluso si despliegan herramientas similares. En general las acciones del Kremlin están diseñadas para generar desconfianza en los estados a las que se dirigen. La intención del PCC es moldear, manejar, y controlar su entorno operativo a fin de que el sentimiento del público sea favorable o se perciba como favorable a sus intereses, y no simplemente a los intereses de China o del pueblo chino. Este objetivo es fruto de la noción de seguridad estatal desarrollada por el PCC: sus percepciones de una amenaza expansiva lo obligan a ampliar su poder más allá de las fronteras de la RPC. Hay cada vez más pruebas de peso de que el régimen pretende utilizar la recolección masiva de datos para apoyar acciones de control de su entorno operativo mundial. Entre otras aplicaciones, los datos recabados servirían de base para elaborar instrumentos destinados a moldear el discurso público en el exterior.[39]

En el marco de su estrategia de seguridad el régimen unipartidista chino se prepara para todo tipo de crisis, desde disturbios sociales a gran escala, desastres naturales y emergencias como las de la pandemia de COVID-19, hasta conflictos armados con fuerzas militares extranjeras como en el caso de Taiwán o de los territorios en disputa del mar de China Meridional. No obstante, el PCC es al mismo tiempo extremadamente cauteloso en lo relativo a noticias, informaciones, opiniones, o debates que contradigan su propia versión de la verdad y que puedan deslegitimar o desestabilizar a su gobierno. Esta preocupación

es, en parte, el motivo por el cual en China hay varios libros blancos sobre cuestiones de defensa que hacen referencia a "señales de un aumento de la hegemonía, de la política del poder y del neointervencionismo"[40] o a la idea de que China "se enfrenta a maniobras estratégicas y a acciones de contención provenientes del exterior al tiempo que debe afrontar en su interior situaciones de perturbación y de sabotaje causadas por fuerzas hostiles y separatistas."[41] La percepción de una amenaza se ve ampliada aún más cuando la tecnología se percibe como un mecanismo para organizar o apoyar una "revolución de color" (un movimiento cívico impulsado por protestas en pro de una transición a la democracia). Esta percepción del riesgo sirve para explicar conceptos desarrollados por el PCC como el de la soberanía del ciberespacio, que no solamente tienen que ver con la protección del entorno físico o de internet en el ámbito interno, sino que representan el control de un espacio de ideas ilimitadas que trasciende toda frontera.[42]

El PCC no separa su estrategia de seguridad en componentes nacionales e internacionales, dado que tanto las amenazas políticas como ideológicas que percibe pueden provenir del exterior. El régimen considera que las revoluciones de colores son parcialmente provocadas por "fuerzas hostiles" externas a la RPC. En 2000 Jiang Zemin, quien por ese entonces era el líder de la RPC, pronunció un discurso en el que alertó que "la internet se ha transformado en un nuevo e importante frente del trabajo político e ideológico. Existen fuerzas hostiles en el país y en el exterior que hacen todo lo posible para utilizarla para competir con nuestro partido y gobierno por las masas y la juventud. Debemos estudiar sus características y adoptar medidas efectivas dirigidas a hacer frente a este tipo de desafío. Es preciso que tomemos la iniciativa a efectos de aumentar nuestra influencia y propaganda positiva en internet."[43] La maquinaria propagandística internacional y en línea del PCC se ha ampliado considerablemente desde esos años, en particular en la administración de Xi Jinping. Esencialmente la seguridad estatal de la RPC es en realidad la seguridad del partido, independientemente de las fronteras del Estado, en especial en lo relativo a los ámbitos ideológico y político.

A fin de ilustrar la naturaleza fluida e imbricada de estas ideas en el seno del PCC, en una alocución pronunciada en 2018 Xi Jinping expresó que "la finalidad de la seguridad estatal es la seguridad del pueblo, la seguridad política es la raíz de la seguridad estatal, la supremacía de los intereses nacionales es el criterio de la seguridad estatal, la consecución de la dicha popular, la gobernanza del partido a largo plazo, y la estabilidad perdurable del país."[44] En otras palabras, según un artículo originalmente publicado en el *People's Liberation Army Daily*, la seguridad política "se refiere al estado objetivo de la soberanía estatal, del poder, sistema y orden políticos, y a una ideología que se halla protegida de las amenazas, infracciones, subversiones, y acciones de destrucción."[45] Reiteramos que el concepto de seguridad estatal no tiene que ver con la protección

Estudio de caso: El gran potencial de los macrodatos

En un informe publicado en 2019, *Engineering Global Consent*, se presentó el perfil de una compañía denominada Global Tone Communications Technology (GTCOM), controlada por el Departamento Central de Propaganda.[46] GTCOM, que se describe a sí misma como una empresa de "macrodatos multilingües," indica que recaba datos en forma masiva en más de 65 idiomas y procesa la información que sirve como insumo de otros productos y servicios para clientes del ámbito gubernamental y empresarial. En términos de escala GTCOM señala que recopila anualmente hasta dos o tres petabytes de datos, el equivalente de aproximadamente 20 millones de fotos en Facebook. En palabras de Liang Haoyu, director de macrodatos de la empresa, "GTCOM intenta reforzar su [capacidad] de reconocimiento de objetos, entornos, y rostros humanos, junto con textos y voces, a fin de brindar una supervisión de los riesgos de seguridad en tiempo real. En el futuro [GTCOM] podrá individualizar la estructura facial solicitada mediante el reconocimiento de imágenes, además de prestar apoyo y soporte técnico para la seguridad estatal."[47] Una presentación efectuada por el Sr. Liang en 2017 contenía una imagen proyectada a su lado con el siguiente texto: "El 90 por ciento de los datos de inteligencia de uso militar puede obtenerse por medio de un análisis de datos abiertos."[48]

El propósito final del uso de toda esta información que se recaba no queda totalmente claro. En cierta medida el PCC recopila datos en forma masiva y después se preocupa de lo que hará con ellos, ya que prevé una mayor capacidad técnica para explotar ese caudal informativo a futuro. No obstante, más allá de las expresiones del Sr. Liang sobre las posibles aplicaciones en materia de seguridad, resulta revelador que GTCOM se encuentre bajo la égida del Departamento Central de Propaganda. La estructura sugiere la intención de desarrollar nuevas herramientas, como comentarios, imágenes, y videos en medios sociales de carácter ficto generados por mecanismos de inteligencia artificial, que podrían facilitar la manipulación del discurso público y fomentar el programa de poder incisivo del PCC.

de China y de su pueblo en forma separada de la dirigencia del partido. La seguridad estatal implica la protección del régimen del PCC por sobre todo lo demás.

Para moldear la percepción pública de modo efectivo hay que comprender el sentimiento público. En este sentido la metodología del PCC no es muy distinta de la que se utiliza en el sector publicitario internacional, salvo que en lugar de procurar la venta de un producto el partido trata de promover el control y el gobierno autoritario más allá de las fronteras de la RPC. En 2013 Jiang Jianguo, quien en ese entonces era secretario del partido y subdirector de la antigua Administración Estatal de Prensa, Publicaciones, Películas, y Televisión, expresó que era preciso comprender la "psicología y los hábitos de aceptación de los públicos extranjeros" a efectos de que la RPC lograra "consolidar la elaboración e innovación de los contenidos comunicativos" y "hacer realidad una comunicación focalizada dirigida a públicos diversos" "de forma tal que las imágenes, sonidos, textos, e información de los medios masivos tradicionales de [China] puedan difundirse ampliamente en todo el mundo."

Las tecnologías emergentes, en particular las que utilizan macrodatos, constituyen un componente esencial de las actividades del PCC dirigidas al conocimiento y a la manipulación de sus públicos internacionales. Los grandes conjuntos de datos pueden revelar pautas y tendencias del comportamiento humano, además de permitir un análisis de sentimientos más preciso que, entre otras cosas, podría serle útil al régimen unipartidista para difundir su propaganda de modo más eficaz.

Si bien las mencionadas estrategias de propaganda basadas en datos aún se hallan en etapa de desarrollo, el régimen ya se encuentra intensificando sus acciones generales dirigidas a moldear la opinión pública internacional, lo que demuestra al menos una voluntad política que en poco tiempo podría dar paso a medios más avanzados para ponerlas en práctica. Por ejemplo, en junio de 2020 Twitter informó que había eliminado cuentas que, según dijo, eran parte de una campaña encubierta de influencia con respaldo estatal. La empresa suprimió varias cuentas ligadas a la RPC que mayormente publicaban desinformación sobre el movimiento democrático hongkonés, sobre el multimillonario con sede en Estados Unidos Guo Wengui (en particular en cuanto a su relación con Steve Bannon, quien fuera asesor de la Casa Blanca) y, en menor medida, sobre el COVID-19 y Taiwán.[49] Aunque la campaña no tuvo un nivel de complejidad muy alto hay señales que apuntan hacia un avance en esa dirección. Los indicadores de esta realidad incluyen, entre otros, el hecho de que presuntamente la empresa Global Tone Communications Technology (ver el recuadro), controlada por el PCC, ha presentado solicitudes de patentes relativas a un método de traducción automatizada que utiliza redes generativas adversarias (GAN, por sus siglas inglesas). Las GAN pueden usarse para sintetizar imágenes basadas en inteligencia artificial o para el reconocimiento visual del habla con el objeto de la lectura de labios y la producción de voz. Se trata del mismo tipo de tecnología comúnmente asociado con los medios sintéticos, que también se conoce como "ultrafalsos" (*deep fakes*).

ESTABLECIMIENTO DE NORMAS A NIVEL NACIONAL Y MUNDIAL

El objetivo del PCC es reconfigurar la gobernanza mundial. Su expectativa es que la tecnología potencie la complejidad de sus acciones. Utiliza al capitalismo para acceder a los datos que lo puedan ayudar a perturbar los procesos democráticos y a crear un entorno mundial más favorable a su propio poder y seguridad. Además de acumular datos, el régimen unipartidista intenta ser vanguardista en cuanto a las nuevas tecnologías, además de sentar las bases técnicas de nuevas industrias que el resto del mundo tendrá que adoptar. Los actores de las democracias liberales suelen pensar que las nuevas tecnologías son esencialmente neutrales, que son simples herramientas, y que pueden controlar los riesgos derivados de su adopción. El PCC parece entender que no resulta posible que el usuario elimine los aspectos inherentes del diseño tecnológico y que la dominación de las fases iniciales del desarrollo puede rendir frutos durante mucho tiempo.

El gobierno y los institutos de investigación colaboran con las empresas en comités técnicos de normas nacionales con el propósito de estandarizar el desarrollo de los equipos, así como de los requisitos que deben cumplir las empresas a fin de presentar ofertas exitosas en un proyecto.

Los países, empresas u organizaciones no gubernamentales generalmente elaboran normas internacionales en materia tecnológica a fin de establecer parámetros para su uso seguro y reducir los posibles costos de comercialización y fabricación. Dado que es posible que se produzca un aumento de los costos debido a que las tecnologías deben adaptarse para cumplir con las nuevas normativas, puede suceder que los actores entren en competencia para ser los primeros en sentar sus normas. El establecimiento de normas tecnológicas mundiales por medio de organizaciones internacionales, tal como la Organización Internacional de Normalización (International Organization for Standardization, ISO), suele implicar "normas de facto basadas en el mercado" que se corresponden con los objetivos de empresas como Huawei, así como normas gubernamentales como las implantadas internamente en la RPC o en cualquier otro país.[50] El plan denominado Normas de China 2035 prevé la exportación al mundo de las normas de la RPC en materia de tecnologías emergentes y la aceptación de las normas chinas a través de los órganos de normalización.[51] De producirse la aceptación internacional de las normas técnicas originadas en la RPC, en especial de las relativas a aspectos clave de la infraestructura técnica, los sistemas elaborados en China gozarán de una mayor interoperabilidad y acceso al mercado en el resto del mundo. El problema para las democracias es que las normas de la RPC fueron diseñadas con un doble propósito: garantizar la calidad e interoperabilidad de los diferentes equipos y lograr que la tecnología facilite los objetivos de gestión social sumamente politizados del régimen unipartidista.[52]

En el ámbito nacional la investigación y el desarrollo en materia tecnológica se realizan con el objeto de satisfacer las necesidades del PCC, que generalmente se asientan en documentos gubernamentales de normalización. A lo largo y a lo ancho de China se encuentran cientos de productos de empresas que se utilizan en los proyectos de las ciudades inteligentes, lo cual hace que la implementación se perciba como caótica y dispareja. No obstante, el hecho de que la normalización se efectúe a nivel del diseño indica que es posible lograr una interoperabilidad fluida entre los diversos sistemas de las ciudades inteligentes. El gobierno y los institutos de investigación colaboran con las empresas en comités técnicos de normas nacionales con el propósito de estandarizar el desarrollo de los equipos y los requisitos que deben cumplir las empresas para presentar ofertas exitosas en un proyecto. Por ejemplo, el documento GA/T1334 de 2015 relativo a los requisitos técnicos para el reconocimiento facial en sistemas de seguridad se elaboró con la cooperación de más de doce entidades, entre las que se encontraban institutos de investigación como la Academia China de Ciencias, la Universidad Nacional de Tecnología de Defensa, y el Primer Instituto de Investigación del Ministerio de Seguridad Pública, empresas tecnológicas como Hikvision y Dahua, y órganos de seguridad pública como el Departamento Provincial de Seguridad Pública de Shanxi y la Oficina de Seguridad Pública de Wuhan.[53] Este tipo de documentos se utiliza como base de los requisitos técnicos en los contratos de compras públicas.

En la práctica los gobiernos locales de la RPC aún no han podido lograr una interoperabilidad fluida entre los departamentos gubernamentales ni con otras administraciones locales mediante plataformas de ciudades inteligentes, lo cual no implica que ese objetivo seguirá siendo

inalcanzable. El establecimiento de normas y la exigencia de su cumplimiento por parte de quienes presentan ofertas en los proyectos aumentan la probabilidad de que los planes como Skynet y Ojos Atentos logren una mayor cohesión y se pongan en práctica con éxito, a pesar de los muchos partícipes. Esta misma lógica se aplica en el ámbito internacional. Si bien la RPC no puede imponer sus normas a otros países, puede favorecer el establecimiento de normas que se tornen internacionales dirigidas a facilitar la adopción mundial de sus tecnologías, integrar efectivamente los valores políticos del PCC y potenciar la capacidad del régimen de aprovechar sus ventajas y proyectar su poder incisivo.

Resulta tentador desestimar la viabilidad del plan del gobierno chino de utilizar la tecnología de las ciudades inteligentes como mecanismo de vigilancia del movimiento de grandes poblaciones. Los problemas que tuvieron los gobiernos locales para potenciar dichos sistemas a fin de dar respuesta al brote del COVID-19 a inicios de 2020 son un ejemplo de que en la actualidad las posibilidades de integración de datos de fuentes diferentes son limitadas. Según el *Financial Times*, algunas empresas privadas se rehusaron a compartir los datos de localización de sus usuarios (que se consideran de mayor calidad que los que poseen las compañías estatales de telecomunicaciones) solicitados por los gobiernos locales para realizar el rastreo y seguimiento de personas de alto riesgo.[54] No obstante, resulta erróneo concentrarse en las deficiencias actuales en vez de en la trayectoria a largo plazo ya que, entre otras razones, las brechas reveladas por la crisis del COVID-19 podrían acelerar las mejoras y, en última instancia, aumentar el nivel de eficiencia de la tecnología. Una vez que la tecnología se ponga a la par de las ideas la implementación de esas demandas de datos será cada vez más automatizada.

En definitiva las empresas privadas no tienen la facultad propia de rehusarse a cumplir las demandas de datos efectuadas por el gobierno de la RPC.[55] La concepción de seguridad estatal de la RPC implica que todos son responsables de prevenir y detener conductas que comprometan la seguridad del Estado chino, independientemente del lugar del mundo en el que se encuentren.[56] La serie de normas legales en materia de seguridad difundidas por el régimen de Xi Jinping resulta sumamente clara en este sentido. Por ejemplo, el artículo 7 de la Ley Nacional de Inteligencia dispone que "toda organización y ciudadano, de conformidad con la ley, deberá prestar apoyo, ayuda, y cooperación en las tareas de inteligencia nacional, además de mantener el carácter secreto de todo producto de inteligencia de que tome conocimiento." Existe en China una corriente que propugna el aumento de la seguridad de los datos, lo cual ha quedado ejemplificado con la publicación en octubre de 2020 del proyecto de la Ley de Protección de Información Personal (LPIP) que propone la adopción de medidas relativas al consentimiento y a los derechos individuales, al reconocimiento facial, a las responsabilidades de quienes manejan los datos, y a las restricciones del procesamiento de ciertos datos personales.[57] Puede decirse que en la actualidad las empresas comerciales hacen muy poco para proteger la privacidad de la persona, por lo que resulta necesario que el gobierno tome más medidas dirigidas a reglamentar la protección de dicha privacidad. No obstante, eso no significa que esas protecciones vayan a limitar el poder del partido. Dado que el régimen unipartidista describe a la ley como un instrumento cuyo objetivo supremo es garantizar la seguridad política del partido, la independencia que puedan tener las empresas de la RPC para resistir la presión política se encuentra obviamente restringida. Xi Jinping expresó que "basarse integralmente en la ley para gobernar el país no debilita en medida alguna a la dirigencia del partido," sino que consolida la posición constituida del partido en el poder.[58]

Estos factores permanecerán inalterados incluso con la internacionalización gradual de las empresas chinas o la procura continua de las compañías extranjeras de acceder a los mercados de la RPC. En noviembre de 2020 el *Wall Street Journal* informó que un exejecutivo de Airbnb había presentado su renuncia debido a que la empresa había compartido datos de los usuarios con funcionarios chinos. El artículo noticioso indicaba que en 2019 las autoridades chinas se habían "presentado a Airbnb una solicitud no escrita en la que pedían más datos de usuarios, incluida una

mayor cantidad de "datos en tiempo real," como por ejemplo el primer momento en que el usuario realiza una reservación.[59] En relación con esta cuestión cabe señalar que en diciembre de 2020 fiscales del Departamento de Justicia presentaron una denuncia relativa a un empleado de Zoom que compartió información de usuarios con funcionarios de seguridad chinos y cortó videollamadas organizadas por personas ubicadas fuera del territorio chino referentes al aniversario de la masacre de 1989 en la Plaza Tiananmén.[60] No es posible creer que si la RPC tiene la capacidad de coaccionar a las compañías extranjeras para que compartan sus datos las empresas ubicadas dentro de sus fronteras cuentan con una facultad firme para resistirse.

La RPC participa activamente en los organismos internacionales de normalización técnica de las tecnologías emergentes, incluidas las de 5G, internet de las cosas, e inteligencia artificial. La intervención china en estos espacios y la relativa ausencia de participación de las democracias liberales se traduce en una ventaja para la RPC frente a sus competidores, además de darle a Beijín la posibilidad de moldear las normas internacionales que sirven a sus intereses políticos.[61] El gobierno de la RPC mantiene una sólida presencia en la Unión Internacional de Telecomunicaciones (UIT), que utiliza para "inclinar el programa de normalización a favor de Huawei."[62] Asimismo, China ha desempeñado un papel de importancia en la ISO y en la Comisión Electrotécnica Internacional (CEI), dos de las entidades de normalización técnica más grandes del mundo. Según el Consejo Empresarial Chino Estadounidense, la cantidad de secretarías ocupadas por la RPC en comisiones y subcomisiones técnicas registró un aumento del 73% en la ISO (entre 2011 y 2020) y de 67% en la CEI (entre 2012 y 2020).[63] Mediante su presencia en los mencionados organismos la RPC moldea directamente las normas relativas a diversas materias.[64] Incluso sin esta participación directa las empresas chinas fijan normas predeterminadamente mediante la exportación de sus productos a todo el mundo. Las empresas de la RPC como Hikvision y Dahua dominan el mercado internacional de las cámaras de seguridad, aunque en los últimos tiempos se ha producido una baja en las ventas por las sanciones impuestas por Estados Unidos debidas a que proporcionan tecnologías de vigilancia que permiten la represión de la población uigur de Xinjiang.

El problema se percibe más claramente cuando los gigantes tecnológicos chinos reciben certificaciones por haber cumplido las normas internacionales que ayudaron a establecer. La empresa YITU, por ejemplo, proporciona programas informáticos de reconocimiento facial y control del tráfico a los proyectos de ciudades inteligentes de Huawei y es considerada una de las "campeonas de la inteligencia artificial."[65] Un comunicado de prensa de la empresa de julio de 2020 señala que la Institución Británica de Normalización confirmó que YITU cumplió los requisitos para la certificación ISO/IEC 27701:2019 en lo referente a sus sistemas de manejo de información personal identificable. La empresa indicó que eso indicaba su observancia de "una certificación internacional de amplia aceptación correspondiente a sistemas de manejo de información de privacidad (PIMS, por sus siglas inglesas) que cumplen las mejores prácticas delineadas en normativas tales como el Reglamento General de Protección de Datos (RGPD) [de la Unión Europea][66] No obstante, YITU participa directamente en el sistema de represión implantado por el régimen unipartidista en Xinjiang. Según el proyecto *Mapping China's Technology Giants* (Mapeo de los Gigantes Tecnológicos de China) que lleva adelante el Australian Strategic Policy Institute (Instituto Australiano de Política Estratégica), YITU apoya las tareas de seguridad pública en Xinjiang mediante su sistema de retratos dinámicos, además de cooperar con otras empresas de la región en cuestiones de seguridad pública.[67] Una investigación del *New York Times* puso de manifiesto que la base de datos generada por YITU incluía códigos para identificar a uigures a partir de imágenes de videos de seguridad pública.[68] El informe periodístico sugiere que YITU cumple con varias normas, como la GA/T1314, que asigna campos para la codificación de la nacionalidad e identidad étnica de la persona. Aunque existen motivos claros para cuestionar si los valores de la empresa se alinean con los propósitos de las normativas como la RGPD, hasta hace muy poco este problema quedó mayormente ignorado.

Es preciso que las democracias liberales logren explicar a sus públicos los motivos por los cuales el autoritarismo chino potenciado por la tecnología constituye una amenaza sistémica directa que, entre otros efectos, menoscaba la libertad de expresión y la autonomía de la persona.

ARTICULACIÓN DE IDEAS Y VALORES DEMOCRÁTICOS QUE RIJAN LA TECNOLOGÍA

Tanto para los investigadores como para los encargados de la toma de decisiones y para la sociedad civil resulta esencial lograr una comprensión profunda y específica del país de que se trate en cuanto a los mecanismos utilizados por sus actores estatales—como el gobierno de la RPC—para proyectar el poder incisivo mediante las nuevas tecnologías. Dado que la actuación de los estados difiere según sus intereses e intenciones, las consecuencias del poder incisivo potenciado por la tecnología varían. Aunque los enfoques de políticas "agnósticos en cuanto al país" en materia de toma de decisiones parezcan más objetivos, suelen ocultar importantes realidades al no definir adecuadamente la naturaleza del problema. Las distintas intencionalidades de los actores autoritarios afectan diferentes esferas y exigen respuestas específicas.

Al mismo tiempo es preciso que las democracias liberales logren explicar a sus públicos los motivos por los cuales el autoritarismo chino potenciado por la tecnología constituye una amenaza sistémica directa que, entre otros efectos, menoscaba la libertad de expresión y la autonomía de la persona. Al hacerlo, las democracias liberales deben dejar muy en claro las razones por las que la alternativa que ofrecen es mejor. Deben expresar sin ambages lo que implican los valores democráticos liberales e invertir en su protección. Dado el alcance multisectorial del desafío, la sociedad civil tiene la posibilidad de desempeñar una función singular y fundamental mediante acciones de coordinación con los medios, con el gobierno, y con los actores del sector privado dirigidas a mitigar los problemas relativos a la proyección de la tecnología y del poder incisivo.

A tales efectos la sociedad civil debe considerar las acciones que se indican a continuación.

1. **Fortalecimiento del discurso público en materia de tecnología y valores democráticos liberales**

   - Es preciso capacitar a las organizaciones de la sociedad civil en temas relativos a las tecnologías emergentes para que puedan ofrecer programas educativos sobre las mejores prácticas de seguridad de los datos. Por ejemplo, podrían diseñarse programas de alfabetización digital que vayan más allá de los métodos básicos personales y empresariales de gestión de datos e incluyan un análisis de la dimensión geopolítica de los temas así como de los mecanismos de abuso de las acciones de recolección de datos aparentemente inocuas. La capacitación en materia de seguridad digital debe incorporarse a los programas internacionales de desarrollo.

   - Las organizaciones mediáticas y de la sociedad civil deben colaborar en forma coordinada a fin de exponer y difundir ampliamente en sus países los indicadores del poder incisivo potenciado por la tecnología, lo que contribuiría a una mayor concientización pública de las cuestiones, incentivaría el debate de las medidas necesarias, y presionaría a los gobiernos para que tomen medidas de protección. Resulta preciso que los equipos de los principales medios investigativos incorporen expertos en técnicas forenses de análisis de datos y otros especialistas en tecnología.

   - Los actores de la sociedad civil deben realizar investigaciones sobre las percepciones públicas en materia de vigilancia digital y de protección de datos a fin de encuadrar las

normas técnicas que deberían establecer los gobiernos de las democracias liberales cuando presentan sus alternativas a las iniciativas autoritarias. La privacidad de los datos constituye un valor común y quizás universal: es posible que las investigaciones sobre la opinión pública en la materia contribuyan a restringir a los gobiernos autoritarios mediante normas sólidas basadas en derechos individuales.

- Los periodistas y las organizaciones de la sociedad civil deben utilizar sus conocimientos de expertos del idioma chino para intensificar sus investigaciones de las leyes, normativas, y pronunciamientos de la RPC a fin de comprender más cabalmente las intenciones del PCC de reconfigurar las tecnologías emergentes que se implementan con regularidad y que sobrepasan las actualizaciones de la normativa internacional.

2. Generación de consenso y coordinación de las respuestas de los socios democráticos

- Toda vez que sea posible es preciso que las organizaciones de la sociedad civil trabajen en coordinación con los gobiernos democráticos y con el sector privado a fin de hallar soluciones de políticas para los desafíos cada vez más complejos y de rápida evolución que imponen las tecnologías emergentes. Deben participar en diálogos significativos a nivel multilateral y de la diplomacia de la Vía 1.5 con el objeto de encontrar respuestas a problemas comunes relativos a la proyección del poder incisivo potenciado por la tecnología. En 2021, por ejemplo, el Instituto Australiano de Política Estratégica tenía previsto ser la sede del Diálogo de Sidney, un encuentro que reuniría a líderes del ámbito político, empresarial, y gubernamental con los mejores pensadores estratégicos del mundo a fin de de realizar debates, generar nuevas ideas, y colaborar para lograr entendimiento común de las oportunidades y amenazas de las nuevas tecnologías.[69]

- Los grupos de la sociedad civil deben participar activamente en los organismos internacionales de normalización, tales como la UIT, la ISO, y la CEI a fin de contribuir a la elaboración de normas rectoras de las tecnologías de 5G y del internet de las cosas, entre otras, y de contrarrestar las acciones lesivas de la RPC que procuran ese mismo propósito. Es preciso que desempeñen un papel en dichos foros junto con los gobiernos y con el sector privado como representantes de los consumidores y de las personas jurídicas. Las organizaciones de la sociedad civil pueden ejercer presión para lograr transparencia en la elaboración de normas técnicas aplicables a las tecnologías que puedan afectar negativamente las libertades civiles, como las de los sistemas de reconocimiento facial o de voz.

- Las empresas tecnológicas de investigación y desarrollo del ámbito empresarial y gubernamental deben invitar a los grupos de la sociedad civil a que las consulten en forma anticipada y frecuente para determinar si sus tecnologías cumplen los criterios democráticos y si deben distanciarse de las normas de la RPC que entran en conflicto con las salvaguardas democráticas.

- Las instituciones de educación superior deben ser responsables de sus propios procesos de debida diligencia relativos a personas físicas, organizaciones, y usos finales de la investigación académica. Es preciso que los comités de ética participen en diálogos significativos con investigadores de derechos humanos y especialistas a fin de elaborar directrices para la evaluación y gestión de los riesgos impuestos por las fuentes de financiamiento y las colaboraciones investigativas vinculadas a regímenes autoritarios en materia de seguridad, reputación y ética.[70]

3. Tratamiento de la inseguridad cibernética en la cadena de suministros

- Las instituciones de investigación, los laboratorios de ideas (*think tanks*), y las demás organizaciones de la sociedad civil de los regímenes democráticos pueden apoyar la elaboración de normativas gubernamentales efectivas en materia de protección y

privacidad de los datos al identificar, consolidar, comunicar, y difundir públicamente los mecanismos oscuros o antidemocráticos de recolección, almacenamiento, e intercambio de datos. Asimismo, las organizaciones de la sociedad civil pueden destinar recursos a la investigación de cuestiones como la seguridad de los datos y las violaciones de la privacidad, particularmente si están asociadas a regímenes autoritarios, y difundirlas de forma generalizada.

- Los investigadores de los laboratorios de ideas, las empresas de inteligencia en materia de seguridad cibernética, y los gobiernos democráticos deben colaborar conjuntamente en investigaciones multianuales que conduzcan a la elaboración de una base de datos de acceso público y de fácil utilización centrada en las cadenas de suministros tecnológicos, en la recolección de datos integrada y en los riesgos correspondientes a la seguridad cibernética. Este recurso debe ponerse a disposición de los gobiernos y de las entidades privadas de forma tal que los desarrolladores de productos o las pequeñas y medianas empresas puedan realizar la debida diligencia de las tecnologías que planean adquirir.
- Es preciso que los actores de la sociedad civil contribuyan a la promoción de estructuras jurídicas más sólidas relativas al uso de los equipos asociados a los proyectos de ciudades inteligentes. Mientras tanto, deben incentivar las inversiones en materia de investigación y desarrollo a fin de ofrecer alternativas fiables a los sistemas y servicios que fueron diseñados para cumplir los criterios de los actores autoritarios. Por ejemplo, podrían apoyar el desarrollo de metodologías de visión computarizada y reconocimiento facial que protejan los derechos a la privacidad, al debido proceso, y a la no discriminación.[71]

Tanto para los investigadores como para los encargados de la toma de decisiones y para la sociedad civil resulta esencial lograr una comprensión profunda y específica del país de que se trate en cuanto a los mecanismos utilizados por sus actores estatales —como el gobierno de la RPC— para proyectar el poder incisivo mediante las nuevas tecnologías.

ENDNOTES

1 Samantha Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion," Australian Strategic Policy Institute, 14 de octubre de 2019, *www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion*.

2 Peter Mattis, "Russian and Chinese Political Interference Activities and Influence Operations," Richard J. Ellings y Robert Sutter, editores, *Axis of Authoritarians: Implications of China-Russia Cooperation* (Seattle, Washington: The National Bureau of Asian Research, 2018).

3 Nadège Rolland, "A 'China Model'? Beijing's Promotion of Alternative Global Norms and Standards," testimonio formulado por escrito para la Comisión de Examen China-Estados Unidos en material Económica y de Seguridad (U.S.-*China Economic and Security Review Commission*), 27 de abril de 2020, *www.nbr.org/publication/a-china-model-beijings-promotion-of-alternative-global-norms-and-standards*; y Liza Tobin, "Xi's Vision for Transforming Global Governance: A Strategic Challenge for Washington and Its Allies," *Texas National Security Review* 2.1 (noviembre de 2018), *http://dx.doi.org/10.26153/tsw/863*.

4 Richard P. Suttmeier, "Assessing China's Technology Potential," *Georgetown Journal of International Affairs,* 5.2 (Verano/otoño de 2004), 97-105, *www.jstor.org/stable/43134293*; Joe McReynolds, editor, *China's Evolving Military Strategy* (Washington, D.C.: The Jamestown Foundation, 2017); y Marcel Angliviel de la Beaumelle, Benjamin Spevack y Devin Thorne, *Open Arms: Evaluating Global Exposure to China's Defense Industrial* Base, C4ADS, octubre de 2019, *www.c4reports.org/open-arms*.

5 Danielle Cave y colaboradores, "Mapping China's Tech Giants," Australian Strategic Policy Institute, 18 de abril de 2019, *www.aspi.org.au\report\mapping-chinas-tech-giants*. Véanse también los resúmenes de empresas en el sitio web del proyecto Mapping China's Tech Giants del Australian Strategic Policy Institute, disponible en *https://chinatechmap.aspi.org.au/#/companies*.

6 Christopher Walker y Jessica Ludwig, "From 'Soft Power' to 'Sharp Power': Rising Authoritarian Influence in the Democratic World," Christopher Walker y Jessica Ludwig, editores, *Sharp Power: Rising Authoritarian Influence,* National Endowment for Democracy, diciembre de 2017, *www.ned.org/wp-content/uploads/2017/12/Sharp-PowerRising-Authoritarian-Influence-Full-Report.pdf*.

7 Christopher Walker, "What is 'Sharp Power?'", *Journal of Democracy* 29.3 (julio de 2018), *www.journalofdemocracy.org/articles/what-is-sharp-power*.

8 Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion."

9 "What Is a Smart City?" Cisco, *www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/what-is-a-smart-city.html*.

10 Samantha Hoffman, "Managing the State: Social Credit, Surveillance, and the CCP's Plan for China", *China Brief*, 17 de agosto de 2017, *https://jamestown.org/program/managing-the-state-social-credit-surveillance-and-the-ccps-plan-for-china*.

11 Samantha Hoffman, "Programming China: The Communist Party's Autonomic Approach to Managing State Security," Universidad de Nottingham, 29 de septiembre de 2017, *http://eprints.nottingham.ac.uk/48547/*.

12 Dahlia Peterson, "Designing Alternatives to China's Repressive Surveillance State," CSET Policy Brief, October 2020, *https://cset.georgetown.edu/wp-content/uploads/CSET-Designing-Alternatives-to-Chinas-Surveillance-State.pdf*; y Danielle Cave, Fergus Ryan y Vicky Xiuzhong Xu, "Mapping More of China's Tech Giants: AI and Surveillance," Australian Strategic Policy Institute, 28 de noviembre de 2019, *www.aspi.org.au/report/mapping-more-chinas-tech-giants*.

13 Li Zhen, "'*Tianwang' jia 'xueliang' chengxiang gong ping'an*" [Con "Skynet" más "Ojos Atentos" las ciudades y las zonas rurales se encuentran seguras], People's Daily, 11 de octubre de 2017, *http://archive.fo/uEMVC*.

14 Peterson, "Designing Alternatives to China's Repressive Surveillance State"; "'*Xueliang gongcheng' nongcun anfang jiankong jianshexiangmu ni zhi duoshao*" [¿Cuánto sabe usted del proyecto "Ojos Atentos" de supervisión de la seguridad en zonas rurales?], zhongguo anfang zhanlan wang [Red de Exhibición de la Seguridad de China], 19 de diciembre de 2016, *https://archive.vn/UjkDN*.

15 Zhen, "'Con "Skynet" más "Ojos Atentos" las ciudades y las zonas rurales se encuentran seguras"; y Ruan Zhanjiang y Shuai Biao, "'*Xueliang gongcheng' zhi mi ping'an jianshe fanghuwang*" ["Proyecto Ojos Atentos" Elaboración de la red de seguridad], *People's Daily*, 14 de febrero de 2019, *http://archive.fo/m6XIB*.

16 Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion."

17 "Smart Meters," Energy NSW, *https://energysaver.nsw.gov.au/households/understand-your-usage/smart-meters*

18 Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, mayo de 2019, *www.hrw.org/sites/default/files/report_pdf/china0519_web5.pdf*.

19 Por ejemplo, "Langchao ruanjian tiyan dianzizhengwu ji su zhilu" [Inspur en la rápida vía del gobierno electrónico], 28 de octubre 2003, *https://web.archive.org/web/20081122161920/http://news.sohu.com/08/81/news214928108.shtml*; y Tian Doudou, "Huizhi 'shuzi zhongguo' (zoujin youxiu guojiazhongdianshiyanshi)—ji cehui yaogan xinxi gongcheng guojiazhongdianshiyanshi" [Retrato de una "China Digital" (Ingreso al Laboratorio Estatal Clave de Excelencia)—Laboratorio Estatal Clave de Información de Ingeniería en Agrimensura, Cartografía y Teledetección], Fundación Nacional de Ciencias Naturales de China, 30 de marzo de 2006, *http://archive.fo/bxGUw*.

20 Samantha Hoffman, "Grasping Power with Both Hands: Social Credit, the Mass Line, and Party Control," *China Brief*, 10 de octubre de 2018, *https://jamestown.org/program/grasping-power-with-both-hands-social-credit-the-mass-line-and-party-control*.

21 "Suzhou qidong jianshe 'chengshi danao'" [Suzhou comienza la construcción de un "cerebro de la ciudad"], Xinhua, 8 de marzo de 2017, *http://archive.is/wM6OE*; "Neimengguzizhiqu 'zhongguo zhihui chengshi zaijian he xinjian ziangmu mingdan'" [Región Autónoma de Mongolia Interior, "Lista de proyectos de ciudades inteligentes nuevos y en construcción en China"], Red de Ciudades Inteligentes, 18 de agosto de 2016, *https://archive.fo/fZ7hx*; y "Wuhan jiaojing yu huaweigongsi qianshu zhihui jiaotong zhanlüe hezuoxieyi" [La policía de tránsito de Wuhan y Huawei firmaron un acuerdo de cooperación estratégica en materia de transporte inteligente], ITS114.com, 24 de agosto de 2017, *http://archive.is/y6Pvs*.

22 Wu Lixia, "Zhihui jiaotong zai goujian zhihui chengshi zhongdi zhongyao zuoyong" [El importante papel del transporte inteligente en la construcción de una ciudad inteligente], Building Technology Research, agosto de 2019, *www.researchgate.net/publication/335217961_zhihuijiaotongzaigoujianzhihuichengshizhongdezhongyaozuoyong*.

23 Sarah K. White, "What Is Geofencing? Putting Location to Work", CIO, 1 de noviembre de 2017, *www.cio.com/article/2383123/geofencing-explained.html*.

24 Jean Marie Takouleu, "Huawei Sets Up a $1.5 Billion Fund to Boost African Smart Cities," *Afrik 21,* 2 de octubre de 2019, *www.afrik21.africa/en/africa-huawei-sets-upa-1-5-billion-fund-to-boost-african-smart-cities*. Véase asimismo el proyecto Mapping China's Tech Giants del Australian Strategic Policy Institute en el que se documentan decenas de proyectos de ciudades inteligentes en todo el mundo, principalmente dirigidos por Huawei. Disponible en: *https://chinatechmap.aspi.org.au/#/map/f2-Huawei,f6-Smart%20cities*.

25 Joe Parkinson, Nicholas Bariyo y Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, 15 de agosto de 2019, *https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017*.

26 "Egypt, China's Huawei Discuss Electricity Network's Transformation to Smart Grid," Cadena Global de Televisión de China, 4 de septiembre de 2020, *https://africa.cgtn.com/2020/09/04/egypt-chinas-huawei-discuss-electricity-networks-transformation-tosmart-grid*.

27 As Wakama, "Nigerian Government and Huawei Partner on Smart Cities Initiative," IT News Africa, 10 de agosto de 2017, *www.itnewsafrica.com/2017/08/nigerian-government-and-huawei-partner-on-smart-cities-initiative*.

28 El siguiente artículo presenta un análisis de las formas en las que el mayor acceso del gobierno a una combinación de datos quantitativos y cualitativos reduce las oportunidades de lograr una rendición de cuentas democrática: Nicholas D. Wright, *Artificial Intelligence and Democratic Norms: Meeting the Authoritarian Challenge*, National Endowment for Democracy, agosto de 2020, *www.ned.org/wp-content/uploads/2020/07/Artificial-Intelligence-Democratic-Norms-Meeting-Authoritarian-Challenge-Wright.pdf*.

29 Cave, Ryan y Xu, "Mapping More of China's Tech Giants: AI and Surveillance." Nota: la autora no tiene en claro si desde esa fecha el acuerdo se ha materializado o no.

30 "Huawei Safe City Solution: Safeguards Serbia" Huawei, 23 de agosto de 2018, *https://archive.vn/pZ9HO*.

31 Lily Kuo, "Hong Kong Bookseller Gui Minhai Jailed for 10 Years in China," *The Guardian*, 25 de febrero de 2020, www.theguardian.com/world/2020/feb/25/gui-minhai-detained-hong-kong-bookseller-jailed-for-10-years-in-china; y Nate Schenkkan e Isabel Linzer, *Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression*, Freedom House, febrero de 2021, https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf.

32 Turkcell, Huawei Sign Deal on Smart Cities in Turkey," *Daily Sabah*, 23 de octubre de 2018, https://archive.vn/6D9EG; y Can Sezer, "UPDATE 1—Turkey's Turkcell Signs Deal to Use Huawei's Mobile Services," Reuters, 12 February 2020, https://archive.vn/TYsby.

33 Asim Kashgarian y Ezel Sahinkaya, "Analysts: Extradition Treaty between Turkey, China Endangers Uighur Refugees," Voice of America, 7 de enero de 2021, www.voanews.com/a/east-asia-pacific_analysts-extradition-treaty-between-turkey-china-endangers-uighur-refugees/6200467.html.

34 "'Eradicating Ideological Viruses': China's Campaign of Repression against Xinjiang's Muslims," Human Rights Watch, 9 de septiembre de 2018, www.hrw.org/sites/default/files/report_pdf/china0918_web2.pdf.

35 Gareth Browne, "How Turkey is Sending Muslim Uighurs Back to China without Breaking Promise," *The Telegraph*, 26 de julio de 2020, www.telegraph.co.uk/news/2020/07/26/turkey-sending-muslim-uighurs-back-china-without-breaking-promise.

36 Matt Schrader, "Huawei's Smart Cities and CCP Influence, at Home and Abroad," *China Brief*, 19 de junio de 2018, https://jamestown.org/program/huaweis-smart-cities-and-ccp-influence-at-home-and-abroad.

37 Dominic Meagher, "Has Hong Kong's National Security Law Created Secret Police with Chinese Characteristics?", *Strategist*, 14 de julio de 2020, www.aspistrategist.org.au/has-hong-kongs-national-security-law-created-secret-police-with-chinese-characteristics.

38 Sean Coughlan, "UK Universities Comply with China's Internet Restrictions," British Broadcasting Corporation, 9 de julio de 2020, www.bbc.com/news/education-53341217.

39 Tobin, "Xi's Vision for Transforming Global Governance: A Strategic Challenge for Washington and Its Allies."

40 "Zhongguo wuzhuangliliang de duoyanghua yunyong" [El empleo diversificado de las Fuerzas Armadas de China], Oficina de Información del Consejo de Estado de la República Popular China, 2013; y "Zhongguo de guofang (2000)" [La defensa nacional china en 2000], Oficina de Información del Consejo de Estado de la República Popular China, octubre de 2000.

41 "Zhongguo de junshizhanlüe (2008)" [La defensa nacional china en 2008], Oficina de Información del Consejo de Estado de la República Popular China, enero de 2009.

42 Samantha Hoffman, "China's Tech-Enhanced Authoritarianism," testimonio formulado por escrito para la Comisión Especial Permanente de Inteligencia de la Cámara de Representantes de Estados Unidos para la audiencia titulada "Autoritarismo digital de China: vigilancia, influencia y control político," 16 de mayo de 2019.

43 "Jiang Zemin: zai zhongyang sixiangzhengzhi gongzuo huiyi shang de jianghua" [Intervención de Jiang Zemin en la Conferencia Central del Trabajo Ideológico y Político], Base de datos de información sobre la reforma de China, 28 de junio de 2000, www.reformdata.org/2000/0628/5849.shtml.

44 ""Zhenghi anquan shi guojiaanquan de genben" [La seguridad política es la raíz de la seguridad estatal], Qstheory, 20 de abril de 2018, https://web.archive.org/web/20180420123613/http:/www.qstheory.cn/defense/2018-04/20/c_1122716581.htm.

45 Ibid.

46 Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion."

47 "Liang Haoyu: zhongyiyutong 'quanqiu gongkai dashuju' zhu fang anquan fengxian" [Liang Haoyu: los "macrodatos públicos internacionales" de GTCOM "global public big data" ayudan a prevenir los riesgos de seguridad], Global Tone Communication Technology Co. Ltd. (GTCOM), 20 de septiembre de 2017, https://archive.vn/FVJHM; y Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion."

48 Ibid.

49 Jake Wallis y colaboradores, "Retweeting through the Great Firewall," Australian Strategic Policy Institute, junio de 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Retweeting%20through%20the%20great%20firewall_1.pdf.

50 Véase, por ejemplo, Justus Baron y Daniel F. Spulber, "Technology Standards and Standards Organizations: Introduction to the Searle Center Database," Universidad Northwestern, 8 de septiembre de 2015, www.law.northwestern.edu/research-faculty/clbe/innovationeconomics/documents/Baron_Spulber_Searle%20Center_Database.pdf.

51 "Chinese Standards Going Global an Unavoidable Trend," *Global Times*, 28 de abril de 2020, https://archive.is/kfUDG.

52 "Shehui zhili zhinenghua de fazhi lujing" [El camino jurídico de la inteligentización de la gobernanza social], Revista de Ciencia Jurídica, 9 de octubre de 2020, www.fxcxw.org.cn/dyna/content.php?id=14294.

53 Lista completa: Universidad Tsinghua, Primer Instituto de Investigación del Ministerio de Seguridad Pública, Hikvision, Instituto de Automatización, Academia China de Ciencias, Universidad Nacional de Tecnología de Defensa, Instituto de Computación de la Academia China de Ciencias, Beijing Haixin Kejin High-Tech Co., Ltd., Guangzhou Pixel Data Technology Development Co., Shanghai Yinchen Intelligent Identification Technology Co., Ltd., Zhejiang Dahua, Shenzhen Zhongkong Biometrics Co., Ltd., Guangdong Boya Information Technology Co., Ltd., Sichuan Chuanda Zhisheng Co., Ltd., Departamento Provincial de Seguridad Pública de Shanxi, Departamento Provincial de Seguridad Pública de Jiangsu y Oficina de Seguridad Pública de Wuhan.

54 Yuan Yang, Nian Liu, Sue-Lin Wong y Qianer Liu, "China, Coronavirus, and Surveillance: The Messy Reality of Personal Data," *Financial Times*, 2 de abril de 2020, www.ft.com/content/760142e6-740e-11ea-95fe-fcd274e920ca.

55 Zach Dorfman, "Tech Giants Are Giving China a Vital Edge in Espionage," *Foreign Policy*, 23 de diciembre de 2020, https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies.

56 Samantha Hoffman, "China's State Security Strategy: 'Everyone Is Responsible,'" *Strategist*, 11 de diciembre de 2017, www.aspistrategist.org.au/chinas-state-security-strategy-everyone-is-responsible.

57 "Zhonghuarenmingongheguo geren xinxi baohufa (caoan)" [Ley de Protección de la Información Personal de la República Popular China (Proyecto)], NPC Observer, octubre de 2020, https://npcobserver.files.wordpress.com/2020/10/personal-information-protection-law-draft.pdf.

58 "Xi Jinping tan fazhi zuixin jin ju pouxi gaoji ganbu zoushang fanzui daolu yuanyin" [Las últimas citas de Xi Jinping sobre el estado de derecho, un análisis de las motivaciones que llevaron a altos funcionarios a cometer delitos], CPC News, 15 de febrero de 2019, http://archive.fo/gnXxA.

59 Dustin Volz y Kirsten Grind, "Airbnb Executive Resigned Last Year over Chinese Request for More Data Sharing," Wall Street Journal, 20 de noviembre de 2020, https://www.wsj.com/articles/airbnb-executive-resigned-last-year-over-chinese-request-for-more-data-sharing-11605896753.

60 Drew Harwell y Ellen Nakashima, "Federal Prosecutors Accuse Zoom Executive of Working with Chinese Government to Surveil Users and Suppress Video Calls," *Washington Post*, 18 de diciembre de 2020, www.washingtonpost.com/technology/2020/12/18/zoom-helped-china-surveillance.

61 Anna Gross y Madhumita Murgia, "China Shows Its Dominance in Surveillance Technology," *Financial Times*, 27 de diciembre de 2019, www.ft.com/content/b34d8ff8-21b4-11ea-92da-f0c92e957a96.

62 Melanie Hart y Jordan Link, "There Is a Solution to the Huawei Challenge," Center for American Progress, 14 de octubre de 2020, www.americanprogress.org/issues/security/reports/2020/10/14/491476/solution-huawei-challenge.

63 "China in International Standards Setting," Consejo Empresarial Chino Estadounidense, febrero de 2020, www.uschina.org/sites/default/files/china_in_international_standards_setting.pdf.

64 Haley Wu, "ISO/IEC Approved China's Standards Proposal on IoT," Experto Europeo en Normalización en Comisión de Servicios en China (SESEC, por sus siglas inglesas), 22 de febrero de 2019, www.sesec.eu/iso-iec-approved-chinas-standards-proposal-on-iot.

65 Cave, Ryan y Xu, "Mapping More of China's Tech Giants: AI and Surveillance."

66 YITU Technology, "YITU Technology Received ISO/IEC 27701:2019 Certification from BSI, Becomes the First Chinese AI Company to Obtain It," CISION PR Newswire, 1 de julio de 2020, *www.prnewswire.com/news-releases/yitu-technology-received-isoiec-277012019-certification-from-bsi-becomes-the-first-chinese-ai-company-to-obtain-it-301086961.html*; e "ISO/IEC 27701:2019 Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines", Organización Internacional de Normalización, agosto de 2019, *www.iso.org/standard/71670.html*.

67 Véase el resumen de la empresa YITU en el sitio web del proyecto Mapping China's Tech Giants del Australian Strategic Policy Institute, disponible en *https://chinatechmap.aspi.org.au/#/company/yitu*.

68 Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *New York Times*, 14 de abril de 2019, *www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html*.

69 Danielle Cave, "Introducing a New Global Technology Initiative: The Sydney Dialogue," *Strategist*, 23 de diciembre de 2020, *https://www.aspistrategist.org.au/introducing-a-new-global-technology-initiative-the-sydney-dialogue.*

70 Kara Frederick, "Democracy by Design: An Affirmative Response to the Illiberal Use of Technology for 2021," Center for a New American Security, 15 de diciembre de 2020, *www.cnas.org/publications/reports/democracy-by-design*.

71 Peterson, "Designing Alternatives to China's Repressive Surveillance State."

LA *NATIONAL ENDOWMENT FOR DEMOCRACY*

La *National Endowment for Democracy* (Fundación Nacional para la Democracia o NED, por sus siglas en inglés) es una fundación privada sin fines de lucro dedicada al desarrollo y al fortalecimiento de las instituciones democráticas del mundo. La NED entrega más de 1.700 subsidios por año para apoyar proyectos de grupos no gubernamentales extranjeros que trabajan en pos de objetivos democráticos en más de 90 países. Desde su fundación en 1983 la NED sigue a la vanguardia de las luchas democráticas *en* todo el planeta, al tiempo que se ha transformado en una institución multifacética que constituye un centro de actividades, recursos e intercambios intelectuales para activistas, profesionales y académicos de la democracia en todo el mundo.

EL *INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES*

El *International Forum for Democratic Studies* (Foro Internacional de Estudios Democráticos) de la *National Endowment for Democracy* (Fundación Nacional para la Democracia o NED, por sus siglas en inglés) es un centro líder para el análisis y debate de la teoría y práctica de la democracia en el mundo. El Foro complementa la misión central de la NED de colaboración con grupos de la sociedad civil del extranjero en sus acciones de fomento y fortalecimiento democrático al vincular a la comunidad académica con activistas del todo el mundo. Las actividades multifacéticas el Foro responden a los retos de los diversos países ya que brindan un análisis de las oportunidades para la reforma, transición y consolidación democráticas. El Foro procura la consecución de sus objetivos mediante diferentes iniciativas interrelacionadas: la elaboración del *Journal of Democracy* (Diario de la Democracia), publicación líder en el mundo en materia de la teoría y la práctica de la democracia, la realización de programas de intercambio para activistas, periodistas y académicos internacionales que trabajan en pro de la democracia, la coordinación de una red mundial de laboratorios de ideas y la ejecución de una serie de iniciativas analíticas diversas dirigidas a examinar temas fundamentales del desarrollo democrático.

1201 Pennsylvania Ave, NW, Suite 1100 | Washington, DC 20004 | (202) 378-9700 | ned.org

ThinkDemocracy @thinkdemocracy