LA LUCHA GLOBAL ANTE LA VIGILANCIA CON IA

NUEVAS TENDENCIAS Y RESPUESTAS DEMOCRÁTICAS

// STEVEN FELDSTEIN / EDUARDO FERREYRA / DANILO KRIVOKAPIĆ / ed. BETH KERLEY

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

FORUM INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

// **DOCUMENTO DE TRABAJO** / JUNIO DE 2022

LA LUCHA GLOBAL ANTE LA VIGILANCIA CON IA

NUEVAS TENDENCIAS Y RESPUESTAS DEMOCRÁTICAS

ÍNDICE

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

FORUM INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

NOTA DE LA EDITORA

// **BETH KERLEY,** OFICIAL PRINCIPAL DE PROGRAMACIÓN, INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES (FORO INTERNACIONAL DE ESTUDIOS DEMOCRÁTICOS), NATIONAL ENDOWMENT FOR DEMOCRACY

El presente informe marca el lanzamiento de nuestra serie "Transparencia Tecnológica", un conjunto de publicaciones que busca crear procesos nítidos y participativos para el uso de nuevas tecnologías en el ámbito de la política y la gobernanza. Sobre la base de varios talleres de enfoque transversal, tanto sectoriales como regionales, organizados por el *International Forum for Democratic Studies* (Foro Internacional de Estudios Democráticos) de la *National Endowment for Democracy* (Fundación Nacional para la Democracia), la serie analiza distintas iniciativas en un contexto global, como las relativas a ciudades inteligentes, a herramientas de vigilancia biométricas y a sistemas para la toma de decisiones mediante algoritmos. Nuestros colaboradores abordarán las **repercusiones de las nuevas tecnologías para la democracia y los vectores para la participación de la sociedad civil** en su diseño, implementación y funcionamiento.

A partir de presentaciones realizadas en un taller del Foro realizado en noviembre de 2021, el informe explora los desafíos para la protección de principios y procesos democráticos en el marco de las transformaciones forjadas por los sistemas de vigilancia con inteligencia artificial (IA). Las tecnologías de IA permiten que los Gobiernos recaben, procesen e integren una extraordinaria cantidad de datos de actividades que se realizan dentro y fuera del ciberespacio. Analiza asimismo la **difusión de sistemas de vigilancia con IA, sus efectos y la lucha transnacional para instaurar salvaguardas** para el respeto de valores como la privacidad personal, el acceso igualitario a la justicia, la transparencia en el accionar de los Gobiernos y los procesos decisorios participativos. Se presta particular atención a la **dinámica de los regímenes híbridos y de las democracias jóvenes o frágiles** donde, aunque el control de los poderes de vigilancia puede verse debilitado, la sociedad civil aún cuenta con espacio para investigar y objetar el despliegue de ese tipo de tecnologías.

Esta publicación analiza la difusión de los sistemas de vigilancia con IA, sus efectos y la lucha transnacional para instaurar salvaguardas para el respeto de los valores democráticos.

En el ensayo de apertura, Steven Feldstein, investigador principal del Fondo Carnegie para la Paz Internacional evalúa la **expansión global de las herramientas de vigilancia con IA** y las acciones, tanto locales como multilaterales, que están implementándose para establecer reglas aplicables a su diseño, distribución y uso. Con el objeto de ofrecer un contexto más detallado de las formas en las que las organizaciones de la sociedad civil pueden influenciar este proceso normativo, Eduardo Ferreyra, de la Asociación por los Derechos Civiles de la Argentina, analiza las estrategias para **superar algunos obstáculos comunes que se plantean en la investigación y el debate de los sistemas de vigilancia**, en tanto que Danilo Krivokapić, de la *SHARE Foundation* de Serbia, presenta un caso de estudio que muestra los mecanismos utilizados por su organización para señalar a la atención nacional e internacional la instalación de **cámaras inteligentes de Huawei en Belgrado**.

RESUMEN EJECUTIVO

Desde cámaras que identifican los rostros de los transeúntes hasta algoritmos que llevan un registro de la opinión pública en línea, las herramientas asistidas por IA están abriendo nuevos horizontes para la vigilancia estatal en todo el mundo. Las fuerzas del orden, así como las organizaciones de seguridad nacional, justicia penal y gestión de fronteras de todo el planeta se valen cada vez más de estas tecnologías, que recurren al reconocimiento por patrones estadísticos, al aprendizaje automático y al análisis de macrodatos para clasificar la información y predecir autónomamente las pautas resultantes. ¿Cuáles son las consecuencias para la gobernanza generadas por esta mayor capacidad de vigilancia?

Los principios democráticos peligran si no se pone coto a la vigilancia con IA

La ausencia de salvaguardas jurídicas y técnicas adecuadas hace que las herramientas de vigilancia con IA planteen diversos riesgos para la privacidad, el estado de derecho y la igualdad. Al habilitar la supervisión pública omnipresente, dichas herramientas pueden **facilitar la represión sistemática de grupos específicamente identificados, alentar la extralimitación investigativa o tener un efecto paralizante en los derechos de expresión y asociación**. Estas capacidades se están poniendo a prueba hasta el límite en la República Popular China (RPC), donde se perfila una infraestructura de autoritarismo digital sumamente compleja. No obstante, también presentan considerables desafíos en entornos en los que la ciudadanía goza de cierta libertad política.

El mercado mundial de los sistemas de vigilancia con IA incluye autocracias estrictas, democracias liberales y una cantidad cada vez mayor de “estados pendulares” que ocupan el espacio intermedio. La RPC ha surgido como uno de los principales proveedores de este estas tecnologías. Sin embargo, en todo el mundo, con una leve diferencia para las democracias respecto de los sistemas autocráticos, los Estados cuentan con capacidades de vigilancia con IA, y los proveedores con sede en países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) venden estos sistemas a regímenes de todo tipo.

En los estados pendulares, que combinan características de la democracia y de la autocracia, los vacíos en el estado de derecho y la fragilidad democrática intensifican el riesgo de que se cometan abusos mediante los sistemas de vigilancia. Como la demanda interna se enfrenta a exportaciones a bajos precios desde la RPC, los países de esta categoría adquieren cada vez más sistemas de vigilancia con IA, a pesar de que se ha demostrado que estas tecnologías no responden a las expectativas en cuanto a sus efectos en la seguridad pública.

Las partes interesadas deben colaborar a efectos de proteger los derechos humanos

A nivel mundial las estrategias de IA de los Gobiernos nacionales no abordan de modo suficiente los efectos sobre los derechos humanos. No obstante, las repercusiones de las herramientas de vigilancia con IA se están incorporando a las agendas de la UE y de foros multilaterales como la Organización de las Naciones Unidas (ONU) y la OCDE. A medida que en el mundo las sociedades despliegan esfuerzos para normar tecnologías específicas (como el reconocimiento facial) y la inteligencia artificial en general, resulta fundamental que todos los sectores colaboren a fin de proteger los principios y procesos democráticos. Las entidades del sector privado deberían tomar mayores iniciativas para evaluar los efectos de sus productos en los derechos humanos y desarrollar salvaguardas adecuadas. Mediante su función de órganos de control, de generadoras de conciencia y de creadoras de un nuevo entorno normativo, las organizaciones de la sociedad civil (OSC) de todos niveles son clave para asegurar la rendición de cuentas.

A continuación se indican algunos aspectos que las sociedades abiertas deberían tener en cuenta al toman medidas para responder a los desafíos planteados por la vigilancia con IA.

- Es necesario que los Gobiernos **dejen de promover principios de IA generales y establezcan raseros, regulaciones y órganos de fiscalización específicos** para garantizar que la IA se utilice de forma congruente con las normas de privacidad y derechos humanos. Los actores de la sociedad civil, actuando en calidad de partes interesadas igualitarias, deberían participar en el proceso normativo en lugar de ser convocados para presentar sus comentarios tras su conclusión.
- La creación de **un organismo multipartito perdurable y responsable de atender cuestiones de vigilancia por tecnologías emergentes** cubriría una brecha importante en el ámbito de las instituciones que elaboran normas de IA. Los Gobiernos y las empresas que integren dicho organismo deberían ajustarse a los criterios más estrictos en materia de prácticas de vigilancia a fin de evitar una debilitación de los principios democráticos fundamentales.

Los actores de la sociedad civil deberían participar en el proceso normativo como partes interesadas de igualitarias.

- La aceleración de los esfuerzos desplegados por Beijín para redactar las reglas de los sistemas de IA implica que las democracias deben **intensificar sus acciones de definición de normas internacionales ajustadas a los principios democráticos**. Las normas de derechos humanos podrían verse afectadas si los experimentos regulatorios y las instancias normativas de la RPC logran delinear la gobernanza mundial en materia de IA. Las iniciativas para la reglamentación de la IA que se desarrollan en Europa representan medidas positivas para contrarrestar las acciones de Beijín.
- Para garantizar que los procesos de gobernanza de la IA sean participativos e inclusivos las sociedades abiertas deben **empoderar a la ciudadanía para que comprenda y evalúe el impacto de los sistemas de inteligencia artificial**, así como la opción de valores que reflejan. Es preciso que la sociedad civil actúe para propugnar la comprensión y la participación de los individuos.

LA LUCHA GLOBAL ANTE LA VIGILANCIA CON IA

// **STEVEN FELDSTEIN,** INVESTIGADOR PRINCIPAL, FONDO CARNEGIE PARA LA PAZ INTERNACIONAL

EL AUGE DE LA VIGILANCIA CON IA

Los adelantos clave que permiten diversas funcionalidades, como el reconocimiento facial, el seguimiento en redes sociales y las técnicas inteligentes para el mantenimiento del orden público, implican que la tecnología de IA está ampliando el poder estatal para el control ciudadano. Si bien las autocracias afianzadas utilizan estas nuevas capacidades con avidez, los sistemas políticos más abiertos también están incorporando la vigilancia con IA, lo que genera alarma en cuanto a sus posibles repercusiones en el debido proceso, la libre expresión y la participación ciudadana activa.

En el contexto del retroceso democrático global, la vigilancia con IA no regulada amenaza con ampliar los vacíos del estado de derecho y favorecer a Gobiernos intolerantes en entornos donde los frenos y contrapesos ya están debilitados. Las campañas de la sociedad civil han señalado estos peligros, y las democracias consolidadas se encaminan hacia una definición de reglas básicas más claras para el uso de la vigilancia con IA. No obstante, la implementación de los principios exige un liderazgo democrático más sólido, además de una colaboración activa entre las partes interesadas y una interacción constante con el público en general.

Los sistemas de IA ofrecen distintos mecanismos que aumentan el poder de vigilancia gubernamental. En primer lugar, facilitan la automatización de las operaciones que antes eran realizadas por seres humanos, por ejemplo mediante algoritmos que compatibilizan imágenes con filmaciones. En segundo lugar, la IA puede clasificar la información y predecir patrones de manera autónoma, lo que permite que los sistemas automatizados marquen las anomalías percibidas y traten de prever hechos futuros[1]. En tercer lugar, los sistemas avanzados de IA logran examinar minuciosamente un volumen extraordinario de datos. Aunque estos elementos benefician a las fuerzas del orden, también **crean riesgos de extralimitación investigativa y de vulneración de la privacidad**, así como un **sesgo discriminatorio** (por ejemplo, cuando las herramientas de reconocimiento registran un mayor índice de identificaciones faciales incorrectas en el caso de sujetos de determinadas razas o etnias). Las comunidades marginalizadas son las que suelen correr con la carga del abuso intencional y del diseño deficiente.

Los riesgos de la vigilancia afectan a todos los tipos de regímenes

En los entornos autoritarios el potencial de estas nuevas tecnologías para intensificar la represión resulta obvio. Cabe destacar que se han hecho investigaciones sobre el **uso combinado de la vigilancia biométrica y el seguimiento en redes sociales a fin de alimentar un sistema integrado de control físico y digital en la provincia china de Xinjiang**[2]. Si bien esta aplicación integral de herramientas de IA para reprimir a toda una región aún representa un caso extremo, el potencial de que los avances en los sistemas de vigilancia socaven las expectativas de privacidad, faciliten la persecución política o la discriminación de grupos y erosionen las libertades de expresión y de asociación no es exclusivo de las autocracias.[3]

El potencial de los avances tecnológicos de vigilancia para socavar o erosionar derechos y libertades no es exclusivo de las autocracias.

En las democracias liberales los promotores de causas sienten una justificada inquietud de que las autoridades utilicen las nuevas tecnologías de modo antidemocrático. En efecto, el uso de la vigilancia electrónica para controlar y acosar a activistas de derechos civiles, a manifestantes y a organizaciones de pueblos nativos estadounidenses, condujo a la sanción de la Ley de Vigilancia de la Inteligencia Extranjera de 1978 de los Estados Unidos, que estableció parámetros la autorización de ciertas actividades de vigilancia electrónica[4]. En la actualidad, dado que la utilización de las herramientas de vigilancia con IA es cada vez mayor y más polémica y que en algunos entornos se registran tendencias de retroceso democrático, los Gobiernos liberales luchan por encontrar un equilibrio aceptable entre mantener el orden público y proteger las libertades civiles.

En **Francia**, el alcalde de Marsella puso en marcha el ***"Proyecto Big Data para la Tranquilidad Pública"*** que incorporará tecnología predictiva para el mantenimiento del orden (a través de la recolección y el análisis de datos en forma masiva con el fin de prever y disuadir posibles actividades delictivas futuras y, en su caso, responder a ellas), además de miles de videocámaras que se le compraron a la empresa ZTE, el gigante tecnológico de la RPC[5]. Según informes recientes, en **Estados Unidos** ya hay entidades públicas que utilizan de manera generalizada la tecnología de reconocimiento facial (TRF), **que incluye programas informáticos desarrollados a partir de la extracción de información de redes sociales realizada por el proveedor privado Clearview AI**[6].

Los departamentos de policía estadounidenses también han recurrido ampliamente a la vigilancia en redes sociales y a los algoritmos de reconocimiento facial para identificar a los sospechosos en el marco de la insurrección en el Capitolio del 6 de enero de 2021[7]. Las fuerzas armadas de Israel están implementando un programa que **integra la TRF con dispositivos de telefonía inteligente o de vigilancia por video para controlar a los palestinos**[8]. En muchos casos la nueva infraestructura de vigilancia se difunde sin ser detectada, y los sistemas sólo llaman la atención pública y son objeto de debate una vez que están instalados.

En las democracias débiles y en los regímenes híbridos los sistemas de vigilancia de avanzada presentan graves riesgos. En los países en los que el retroceso democrático ya ha debilitado los mecanismos de protección del estado de derecho, como Polonia, Hungría, India o Filipinas, estas tecnologías ofrecen **nuevas posibilidades para rastrear e intimidar disidentes, controlar opositores políticos y anticipar desafíos para el poder del Gobierno**[9].

La documentación pública demuestra que estos regímenes están acogiendo los sistemas de vigilancia de alta tecnología. Las autoridades indias utilizan la TRF para localizar a manifestantes[10]. El gobierno serbio celebró un contrato con Huawei para establecer una red de vigilancia que pronto "cubrirá cada calle y pasaje importante" de Belgrado (véase el ensayo de Danilo Krivokapi?, págs. 28–31).[11] **El Gobierno de Pakistán** le compró a la empresa canadiense Sandvine un sistema de vigilancia del tráfico en línea y de supervisión de las comunicaciones por un monto de 18,5 millones de dólares[12].

¿En qué medida la disponibilidad cada vez mayor de los sistemas de vigilancia con IA en los estados pendulares (regímenes híbridos o democracias débiles, definidos a los fines de este informe según los puntajes de democracia electoral de V-Dem) acelera la erosión democrática, alimenta las prácticas represivas o socava el estado de derecho? Es probable que la respuesta a esa pregunta se vea moldeada por las interacciones en el mercado globalizado de sistemas de vigilancia, con China como el principal actor, así como por las condiciones políticas internas de los países que instalan dichos sistemas y los esfuerzos de normativización de la inteligencia artificial desplegados por los Gobiernos nacionales, los grupos de la sociedad civil y la comunidad internacional en general.

La policía en Kuala Lumpur, Malasia, opera un dron. Los oficiales de las fuerzas del orden de todo el mundo utilizan las nuevas tecnologías de vigilancia como herramientas de control social.

EL MERCADO MUNDIAL DE LA VIGILANCIA CON IA

La tecnología de la vigilancia con IA es cada vez más omnipresente, en particular a medida que su costo se reduce y sus componentes pertinentes se tornan más asequibles. Como observa el Índice de IA 2021 de Stanford: **"Las tecnologías necesarias para una vigilancia a gran escala están madurando aceleradamente y las técnicas de clasificación de imágenes, reconocimiento facial, análisis de video e identificación de voz registran un progreso considerable"**[13].

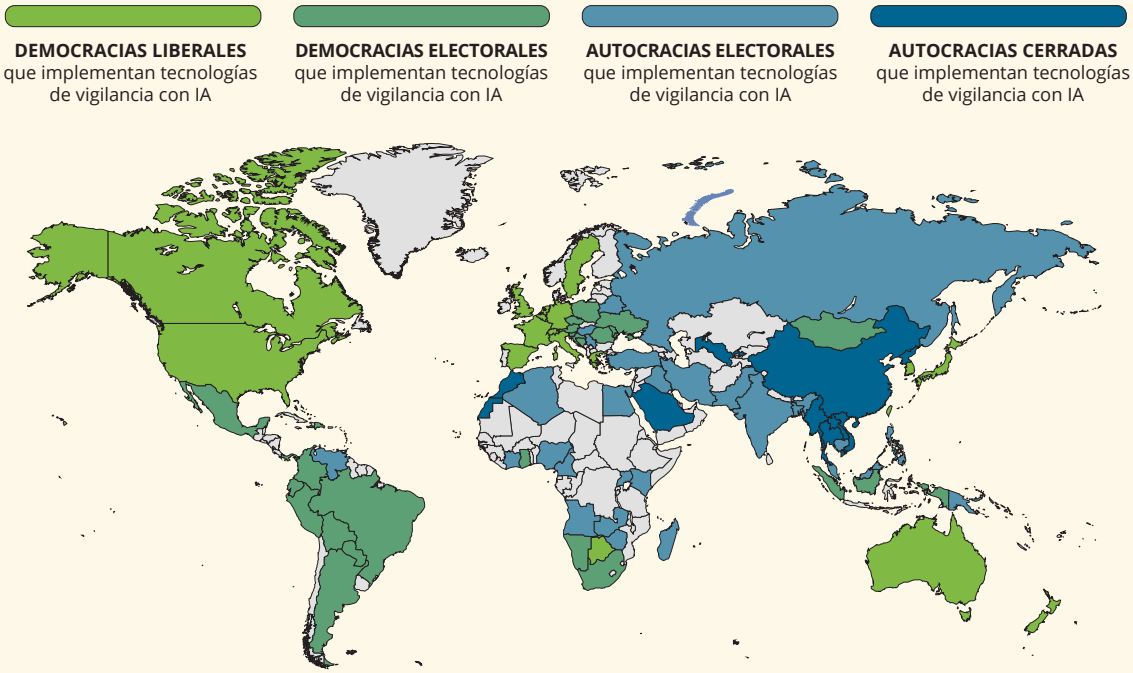
En 2019 publiqué un índice basado en el análisis de contenidos de código abierto para medir la prevalencia mundial de cuatro tipos de sistemas de vigilancia operados mediante IA[14]: TRF (tecnología biométrica que analiza los rostros humanos con fines de identificación), ciudades inteligentes o seguras (redes urbanas con miles de sensores que transmiten datos en tiempo real para facilitar la gestión citadina), técnicas inteligentes para el mantenimiento del orden (métodos basados en datos para la respuesta policial, investigaciones, previsión de delitos e incluso decisiones sobre condenas) y seguimiento en redes sociales (algoritmos que controlan automáticamente millones de comunicaciones en línea). Este índice se actualizó en 2022[15]. Como se muestra en la figura consignada a continuación, por una leve diferencia, hay más Gobiernos democráticos que regímenes

52 de 97

Por una leve diferencia hay más Gobiernos democráticos que regímenes autoritarios con sistemas de vigilancia por IA conocidos.

FIGURA

Presencia de las tecnologías de vigilancia con IA en el mundo

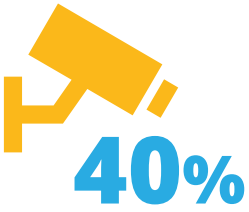


Clasificaciones según el informe de Michael Coppedge y otros, "V-Dem Codebook v12", Proyecto Variedades de Democracia [V-Dem], 2022, págs. 287–88, con datos correspondientes a 2021.

autoritarios con sistemas de vigilancia por IA conocidos: **52 de los 97 países con estas herramientas están clasificados por V-Dem como democracias liberales o electorales**[16].

Las empresas de la RPC son populares proveedoras de herramientas de vigilancia con IA para los Gobiernos.

Las empresas chinas ocupan los primeros lugares en el ámbito del suministro de herramientas avanzadas de inteligencia artificial (IA) y de aprendizaje automático que permiten una vigilancia gubernamental masiva. Estas firmas procuran nuevos mercados en forma activa, y sus acciones suelen recibir apoyo estatal mediante subsidios. Los Gobiernos de todo el mundo se han mostrado muy abiertos a las importaciones a bajo costo posibilitadas por dichos subsidios: en la actualidad las cámaras de vigilancia fabricadas por Hikvision y Dahua representan "casi el 40 %" del mercado mundial[17]. **La tecnología de vigilancia elaborada por china se utiliza en más de ochenta países en todo el mundo**[18].



40%

En la actualidad las cámaras de vigilancia fabricadas por Hikvision y Dahua representan "casi el 40 %" del mercado mundial.

Las exportaciones de los dispositivos de vigilancia chinos se basan en el desarrollo continuo de esas tecnologías en la RPC. A pesar de la indignación internacional por las prácticas de vigilancia en Xinjiang, firmas como Huawei y Dahua trabajan con el Gobierno chino para realizar pruebas piloto con nuevos sistemas que incluyen **programas informáticos para el reconocimiento de emociones** (aplicaciones que procuran deducir el estado emotivo de la persona) y **técnicas de identificación étnica** (programas que usan escaneos faciales para sacar conclusiones sobre la raza) **dirigidos a la población minoritaria uigur de China**[19]. Los investigadores de la organización *Article 19* indican que la RPC cuenta con un "mercado próspero para la tecnología de reconocimiento emocional" con escasa supervisión o consulta pública[20].

Beijín también está consolidando sus capacidades de "fusión de datos" (la combinación de conjuntos de datos dispares para aumentar el poder analítico de las herramientas digitales)[21]. Sus investigadores hacen grandes inversiones destinadas a mejorar los resultados de las técnicas de visión artificial y de vigilancia visual (con especial atención en las de reidentificación de individuos, control de multitudes y detección de robos de identidad facial o *facial spoofing*) o en las utilizadas para determinar si una persona se está haciendo pasar por otra)[22]. **Las autoridades de la RPC también están perfeccionando sus capacidades para la vigilancia masiva de objetivos extranjeros** mediante sofisticados programas informáticos de análisis de datos dirigidos a explotar plataformas externas de redes sociales y de internet[23].

Las empresas ubicadas en países de la OCDE contribuyen activamente al mercado

Cabe notar que las empresas con sede en países de la OCDE también venden programas informáticos de policía predictiva, algoritmos de reconocimiento facial y aplicaciones para la vigilancia en redes sociales, incluso a compradores de regímenes autoritarios. **La mayoría de los Gobiernos, en especial los que cuentan con amplios recursos, evitan deliberadamente depender de un único país o proveedor para cumplir sus objetivos de vigilancia**. Arabia Saudita, por ejemplo, celebró un contrato con **Huawei** para la construcción de ciudades seguras; **Google** y **Microsoft** supervisan los servidores informáticos en la nube del país; **BAE, fabricante de armas del Reino Unido**, ha suministrado sistemas de vigilancia masiva, que incluyeron tecnología de interceptación en internet; **NEC**, de Japón, provee las cámaras de reconocimiento facial; **y Amazon y Alibaba** están considerando una asociación para un importante proyecto de ciudades seguras[24].

La empresa china Hikvision, cuyos productos son cada vez más omnipresentes, es uno de los mayores proveedores mundiales de tecnologías de vigilancia por video.

Hay proveedores europeos y estadounidenses que han exportado herramientas de vigilancia con IA a la RPC, donde se descubrió que algunas de ellas se destinaron a una entidad en Xinjiang[25]. Nótese asimismo que incluso en las democracias liberales se registra un constante aumento en el uso de las tecnologías de vigilancia con IA[26].

La pandemia de COVID-19 fue beneficiosa para los proveedores de sistemas de vigilancia de todo el mundo, ya que los Gobiernos y las instituciones privadas desplegaron aplicaciones de rastreo de contactos, algoritmos predictivos sobre salud pública y sensores de temperatura, entre otras herramientas. Al principio de la epidemia mundial hubo grupos de la sociedad civil que expresaron alarma por los riesgos para la privacidad que implicaba el uso gubernamental de este tipo de sistemas[27]. En efecto, gran cantidad de Estados solo los implementaron en forma parcial o se sintieron decepcionados por los resultados obtenidos[28]. No obstante, existe un **riesgo real de que las medidas invasivas y la erosión de la privacidad de los datos persistan una vez finalizada la pandemia**. En algunos países hay cada vez más indicios de que seguirán utilizándose ciertas herramientas, como el código sanitario de China (una aplicación que mide la probabilidad de exposición del usuario para aprobar su acceso a lugares públicos) lo que podría consolidar nuevos mecanismos de represión política[29]. Las empresas vinculadas con abusos a los derechos humanos en la RPC, como Dahua, tuvieron la oportunidad de expandir sus ventas al exterior gracias a la demanda de dispositivos de escaneo de temperatura [30].

La pandemia de COVID-19 fue beneficiosa para los proveedores de sistemas de vigilancia en todo el mundo.

VULNERABILIDADES DE LOS ESTADOS PENDULARES

Si bien los comentarios se han centrado fundamentalmente en el modelo chino de autoritarismo tecnológico integral o en los debates sobre la vigilancia en entornos liberal demócratas, l**as prácticas de vigilancia con IA pueden afectar seriamente la evolución política de los regímenes híbridos y de las democracias débiles, así como la trayectoria de la normativa tecnológica internacional**[31]. Estos estados pendulares representan entornos políticos parcialmente abiertos en los que las protecciones liberales y democráticas clave están ausentes o se hallan debilitadas, lo que podría acentuar el atractivo de los modelos digitales autoritarios. La implementación de sistemas de vigilancia presenta mayores riesgos para las libertades cívicas y el estado de derecho, aunque queda espacio para que la sociedad civil la cuestione.

Estados pendulares: entornos políticos parcialmente abiertos que combinan rasgos democráticos con atributos autocráticos.

En el presente informe se identifica a los estados pendulares mediante una combinación de puntajes de democracia electoral de V-Dem e indicadores cualitativos seleccionados por el autor, lo que representa un grupo total de 67 países (el listado completo se encuentra en el Apéndice 1)[32]. Si bien todos los estados de esta categoría poseen rasgos democráticos y atributos autocráticos, exhiben variaciones en lo que hace a la solidez de sus marcos de estado de derecho y a los mecanismos a su disposición para la verificación de abusos de los sistemas de vigilancia. La mayoría de ellos registra una variedad de debilidades democráticas graves, como la concentración del poder en el ejecutivo, la falta de independencia judicial, las limitaciones a los medios de comunicación, la represión de la sociedad civil y las violaciones de las libertades políticas.

Los estados pendulares recurren cada vez más a los sistemas de vigilancia con IA

De los 67 estados pendulares, 44 ya poseen capacidades de vigilancia con IA, cifra que aumentará en los próximos años. En muchos casos aún se cuenta con poca información sobre las formas de utilización presente y futura de los instrumentos de IA en estos contextos. No obstante, como he demostrado en estudios anteriores, hay una **estrecha relación entre las restricciones de las libertades políticas y el consecuente abuso gubernamental de las tecnologías de vigilancia**[33]. Por ese motivo existe un muy grave riesgo de que los abusos de los sistemas de vigilancia alimenten y, a su vez, exacerben los problemas de gobernanza generalizados.

44 DE LOS 67
estados pendulares ya poseen capacidades de vigilancia con IA.

¿Cómo deciden los estados pendulares la metodología de utilización de los sistemas de vigilancia con IA? La RPC tiene una importante presencia en la mayoría de estos países, y sus empresas ocupan un lugar destacado en la adquisición e instalación de las tecnologías correspondientes. De los 67 estados pendulares, 55 integran la Iniciativa de la Franja y la Ruta de Beijín. Aun así, **es importante tener en cuenta factores internos, tales como las normas políticas, las amenazas a la seguridad y los incentivos del régimen, que moldean las opciones los Gobiernos** (sin mencionar el efecto de las exportaciones no chinas de tecnologías de IA)[34].

55 DE LOS 67
estados pendulares integran la Iniciativa de la Franja y la Ruta de Beijín

Por ejemplo, los temas de seguridad, ya sean externos o internos, son un elemento importante que impulsa las inversiones en materia de vigilancia. Es lógico que países como India, Pakistán, Iraq y Kenia —que enfrentan diversos desafíos debido a cuestiones de terrorismo, insurgencias internas y grandes influjos de refugiados— opten por invertir en sistemas de vigilancia sofisticados. La influencia de pares también es un factor. Como señala Akın Ünver, las tecnologías de vigilancia a menor costo suministradas por la RPC a ciertos países pueden inducir a estados rivales a "recurrir a los mismos proveedores... con el fin de adquirir rápidamente capacidades concurrentes y resolver sus dilemas de seguridad"[35].

Trayectoria de los sistemas de vigilancia con IA

Un subgrupo de estados pendulares, entre los que se encuentra India, Nigeria y Singapur, muestra indicios de prácticas de vigilancia que generan inquietud en lo que hace a cuestiones de privacidad, justicia o estado de derecho[36]. En India, por ejemplo, las fuerzas policiales recurren sistemáticamente a la TRF para realizar "acciones generalizadas de búsqueda y barrido que suelen efectuase en los barrios pobres densamente poblados por musulmanes e inmigrantes del norte del país"[37]. El avance de la digitalización en India hizo que la vigilancia se incorpore a los mecanismos de gobernanza del país, y llevó a la creación de lo que Sangeeta Mahapatra describe como "un esquema de alerta temprana contra amenazas de seguridad y un sistema moderador del comportamiento para la gestión y control social"[38]. En otros lugares no han surgido o aún no se han documentado patrones de abuso significativos. Los aspectos preocupantes son menos probables en los países con marcos jurídicos sólidos que protegen el **derecho a la privacidad** y brindan **vías para que la ciudadanía exija rendiciones de cuentas**.

Con el fin de llamar la atención del público sobre la instalación de cámaras de Huawei en Belgrado, la *SHARE Foundation* pegó adhesivos en los postes en los que se las había colocado, con la frase "bajo vigilancia" y códigos QR que dirigían a la persona al sitio web de la fundación.

A pesar de su popularidad mundial, **la evidencia sugiere que en muchos países las tecnologías de vigilancia con IA aún no están a la altura de las expectativas**. Si bien esta aparente falencia se debe a una serie de motivos, pueden señalarse cuestiones de capacidad, de disponibilidad de conocimientos especializados y de falta de la interoperabilidad necesaria para el adecuado funcionamiento de estas herramientas de alta tecnología.

A título ilustrativo podemos indicar que aunque en 2016 el Gobierno instaló 8000 cámaras en la ciudad pakistaní de Lahore en el marco de un proyecto de Ciudad Segura, el número total de delitos en Punjab aumentó o no varió en los años subsiguientes[39]. En Kenia hubo inconvenientes legales y obstáculos logísticos que hicieron que una iniciativa de ciudad inteligente tardara trece años en despegar[40]. Según interlocutores, en Filipinas la inversión gubernamental en tecnología de vigilancia china **es gran "teatro de seguridad"** cuyo objeto es la intimidación, aunque no posee un impacto real en la seguridad pública[41]. En palabras de la especialista Sheena Greitens, "la rigurosa evidencia empírica actual del efecto de las plataformas tecnológicas de vigilancia chinas fuera de China es escasa o inexistente"[42]. Redunda en beneficio de investigadores y formuladores de políticas profundizar el estudio de las repercusiones de estas tecnologías en el mundo real.

ESTABLECIMIENTO DE REGLAS DE CONDUCTA

Los estados pendulares y las democracias consolidadas operan actualmente en un entorno en el que aún se están definiendo las normas mundiales generales de vigilancia con IA. **Aunque los foros multilaterales han logrado avances en el establecimiento de un acuerdo sobre principios éticos genéricos en materia de inteligencia artificial, los mecanismos de los Gobiernos o las empresas para incorporar estos conceptos al desarrollo e instalación real de los sistemas de IA aún no están claros.** La preocupación de algunos expertos es que, si las salvaguardas contra el abuso se formulan en términos de "ética de la IA", en lugar de como normas de derechos humanos internacionalmente establecidas, se producirá un vacío jurídico que permitirá que Estados y empresas traten los perjuicios de la IA de modo meramente retórico, sin asumir obligaciones exigibles[43].

La mayoría de las iniciativas en materia de gobernanza de la IA son aún de carácter profundamente abstracto y no presentan detalles para su implementación efectiva.

Iniciativas en materia de políticas gubernamentales y multilaterales para tratar la gobernanza de la IA

Ya existen iniciativas multilaterales, regionales y nacionales para comenzar a abordar las cuestiones de gobernanza de la IA. La mayoría son aún de carácter profundamente abstracto y no presentan detalles para su implementación efectiva. En los últimos tiempos las instituciones regionales europeas han participado activamente en este ámbito. A principios de 2021 la **Comisión Europea presentó la Ley de Inteligencia Artificial**, que propone un marco para atender los riesgos sistémicos de la IA y promover la innovación, y que ya había sido puesta a la consideración del Parlamento Europeo al momento de la elaboración del presente informe en mayo de 2022[44]. Si bien algunas partes interesadas presionan a los legisladores para que prohíban totalmente ciertas categorías tecnológicas, como las herramientas de vigilancia biométrica, lo más probable es que se impongan restricciones, como la exigencia de autorizaciones judiciales o la limitación a la retención de datos. Asimismo, el Consejo de Europa realiza gestiones paralelas para promulgar normas internacionales que rijan la IA[45].

La **Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) ha recomendado una "moratoria" a la venta y uso de "sistemas de IA que presenten un riesgo grave para los derechos humanos"**, mientras se tramitan nuevas salvaguardas[46]. El Consejo de Derechos Humanos de la ONU ha solicitado un informe de seguimiento, que probablemente incidirá en la elaboración de políticas de IA en distintos foros[47]. A mediados de 2021 la **UNESCO** confeccionó una versión preliminar de recomendaciones sobre la ética de la IA, que incluye formulaciones sorprendentemente sólidas en materia de derechos humanos[48].

En términos generales **el enfoque de los Gobiernos nacionales sobre las cuestiones de IA y derechos humanos sigue estando poco desarrollado**, si bien ha habido algunas actividades legislativas en el ámbito local (por ejemplo, la prohibición total de la TRF en la ciudad de Portland, Oregón)[49]. En Estados Unidos se han forjado varias iniciativas nuevas durante la presidencia de Biden. Por ejemplo, la Casa Blanca lanzó un proyecto para elaborar una "declaración de derechos" sobre IA que establecería una nueva normativa para el uso de las tecnologías biométricas y automáticas[50].

Asimismo, Estados Unidos ha implementado **restricciones comerciales a las tecnologías de IA**. Dichas restricciones incluyen la exigencia de permisos para la exportación de tecnologías sensibles, así como la limitación de inversiones en determinadas empresas con sede en la RPC y de transacciones con ellas, debido en parte a los abusos probados de derechos humanos en Xinjiang relativos a las tecnologías de vigilancia con IA[51].

En lo relativo a la proliferación mundial de **estrategias nacionales y regionales de IA**, la empresa *Global Partners Digital* señala que **solo algunos de los documentos que las consagran realizan un análisis exhaustivo de sus efectos en la esfera de los derechos humanos**, además de indicar que la mayoría de ellos no presenta de modo "profundo y específico mecanismos de protección de dichos derechos"[52]. Estas omisiones se contraponen a la exploración detallada de otras cuestiones que constan en los mencionados documentos de estrategia, como la competitividad económica o la promoción de la innovación. En materia de derechos humanos los ámbitos más frecuentemente citados fueron el derecho a la privacidad, seguido del derecho a la igualdad y a la no discriminación. Un subgrupo más pequeño de Estados hizo referencia los derechos a la reparación efectiva, a la libertad de expresión y al acceso a la información[53].

Función de la sociedad civil en la formulación de políticas sobre vigilancia con IA

Las OSC tienen una función esencial en la formulación de políticas sobre vigilancia con IA. **La propensión de las autoridades a tomar decisiones poco transparentes sobre estas cuestiones implica el riesgo de desconsideración de principios de derechos humanos o de aspectos que preocupan a la sociedad.** Resulta fundamental que el público participe en todas las etapas a fin de asegurar que el desarrollo y la implementación de las nuevas tecnologías sigan las orientaciones trazadas por los principios y procesos democráticos.

En primer lugar, **las OSC son necesarias para consolidar la conciencia pública sobre proyectos contratados por el Gobierno que afectan las libertades cívicas**. No es fácil obtener información gubernamental. Eduardo Ferreyra, de la Asociación por los Derechos Civiles de la Argentina, observa que los Gobiernos evitan publicar información contractual sobre tecnologías de vigilancia recientemente adquiridas, y que las solicitudes de acceso a la información sufren demoras o son ignoradas. Aun así, los activistas y periodistas emplean estrategias creativas para superar estos obstáculos y brindar información esencial al público. (Más información en las págs. 25 a 27.)

En la campaña #ConMiCaraNo, la Asociación por los Derechos Civiles advierte acerca de los riesgos de la TRF. El resto del texto dice "No es protección, es control".

En las democracias los ciudadanos tienen más oportunidades para c**uestionar los mecanismos de gasto de fondos públicos, examinar las justificaciones del Gobierno para implementar programas específicos, e indagar el modo en el que los organismos públicos prevén recolectar, almacenar y emplear los datos de los usuarios**. En Filipinas, por ejemplo, la presión de la sociedad civil y de parlamentarios interesados en la problemática logró un importante retraso en el financiamiento de un proyecto de vigilancia contratado con Huawei denominado "Filipinas Seguras"[54]. Danilo Krivokapi? de la *SHARE Foundation* de Serbia relata la forma en que su organización movilizó a la comunidad a raíz de planes de las autoridades para establecer un sistema de vigilancia con tecnología de Huawei en toda la ciudad de Belgrado (véase págs. 28–31). Incluso en algunos entornos más cerrados en los que las OSC cuentan con menos espacio formal de maniobra se registran distintos grupos que han encontrado maneras de lograr indignación pública y ejercer presión para que las autoridades reduzcan o cancelen proyectos preocupantes. En Uganda hubo activistas que advirtieron de los potenciales usos de un proyecto de rastreo digital de vehículos contratado con una firma rusa, teóricamente para combatir el delito[55].

Incluso si los Gobiernos concluyen exitosamente sus proyectos de vigilancia las OSC pueden desempeñar una función fundamental al **"vigilar a los que vigilan" para detectar indicios de abuso**. Los activistas también pueden presionar a las firmas administradoras de estos sistemas para que cumplan principios empresariales y de derechos humanos consagrados (la fuerte reacción pública en contra de las operaciones bielorrusas de Sandvine, una empresa de internet con sede en Canadá, nos ofrece un buen ejemplo)[56]. Por último, aunque muchos Gobiernos y foros internacionales cuentan con procesos de toma de decisiones configurados de manera tal que dificultan los aportes de la sociedad civil, esa

participación es esencial para la formación de normas democráticas. Desde el nivel multilateral hasta el local la ciudadanía puede **presentar informes, asistir a audiencias públicas, realizar peticiones ante legisladores y movilizar a sus conciudadanos para presionar y exigir una mayor rendición de cuentas sobre actividades de vigilancia y restricciones al uso de nuevos sistemas**.

Responsabilidades del sector privado

La responsabilidad de garantizar el cumplimiento de los cánones y normas de derechos humanos no debería corresponderle exclusivamente a los Gobiernos o a las OSC. L**as empresas deberían adoptar ciertas medidas de manera voluntaria para mitigar los daños y proteger la privacidad**. Hay muchas empresas, como la de reconocimiento facial Clearview AI, o las de intermediación de datos como LexisNexis, Nielsen o Acxiom (todas venden "abierta y explícitamente" datos de millones de personas utilizados por los programas informáticos de vigilancia de diversas fuerzas del orden), que desafortunadamente aprovechan los vacíos legales para convalidar sus prácticas comerciales. Resulta paradójico que en Estados Unidos algunos de los clientes más grandes de estas firmas son organismos de cumplimiento de la ley[57]. Justin Sherman, investigador de políticas tecnológicas, señala que "En términos prácticos, ni la industria… ni la práctica de la intermediación de datos se encuentran sometidas a control alguno"[58].

Una solución sería que las legislaturas sancionen leyes sobre privacidad que regulen la operación de las empresas de intermediación de datos y de vigilancia privada, por ejemplo, mediante la determinación de la información que pueden recabar y el establecimiento de mecanismos que permitan que los sujetos afectados procuren una rendición de cuentas. No obstante, **también las empresas tienen de por sí la "responsabilidad de respetar los derechos humanos"**[59]. Los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas disponen la obligación empresarial de evaluar si su conducta constituye una violación de normas procedentes de derechos humanos y de hacer frente a las consecuencias negativas en las que tengan alguna participación[60].

En lo relativo al sector de la vigilancia en particular, en el que el riesgo es mayor, ***Privacy International*** **propone un enfoque útil: acuerdos específicos incorporados en las alianzas público-privadas constituidas entre empresas y Gobiernos** que reflejen principios de transparencia, procesos de compras públicas respetuosos de las normas, rendición de cuentas, supervisión, legalidad, necesidad, proporcionalidad, y desagravio[61]. Esta práctica podría mitigar los aspectos preocupantes que generalmente surgen de estas alianzas, como líneas de rendición de cuentas que suelen desdibujarse y empresas que, aun cuando sus tecnologías son utilizadas por organismos estatales, pueden escudarse en disposiciones de propiedad intelectual y secreto comercial que menoscaban la transparencia de sus operaciones.

RESPUESTA A LA ALTURA DEL DESAFÍO

Las sociedades democráticas aún no han encontrado el conjunto adecuado de salvaguardas que pongan coto a los abusos planteados por los sistemas de vigilancia. No obstante, dado el carácter cada vez más omnipresente de la tecnología de vigilancia con IA, es esencial resolver el estancamiento de políticas y normativas. Como primera medida, los Gobiernos pueden ser más nítidos en el uso de la tecnología de IA. La mejora de la transparencia puede ser tan simple como exigir la presentación **de informes periódicos sobre evaluación de los riesgos de la IA elaborados por los organismos gubernamentales** que implementan esta tecnología, con el objeto de asegurar protecciones adecuadas para la privacidad en las acciones de recolección de datos o de identificar los efectos discriminatorios de conjuntos de datos subyacentes. Esta práctica podría complementarse con evaluaciones previas de las repercusiones para los derechos humanos en casos específicos (por ejemplo, el despliegue de drones operados con IA planificado por las fuerzas del orden para vigilar a las multitudes en las manifestaciones).

Dado el carácter cada vez más omnipresente de la tecnología de vigilancia con IA, es esencial resolver el estancamiento de políticas y normativas.

Los Gobiernos democráticos deberían ir más allá de la promulgación de principios éticos generales sobre la IA y avanzar hacia una **definición de reglamentaciones y criterios concretos para el uso responsable de ese tipo de tecnología que reflejen el derecho y la normativa internacionales de derechos** humanos. Dicha regulación deberá incluir protecciones contra la vulneración de derechos por acciones de rastreo y supervisión masiva, así como límites al uso estatal de conjuntos de datos comerciales a gran escala administrados por intermediarios.

En febrero de 2020 la Comisión Europea celebró una conferencia de prensa sobre inteligencia artificial. Las instituciones europeas han trabajado cada vez más activamente en la definición de normas sobre IA.

La creación de órganos de supervisión, como los grupos de trabajo nacionales para determinar el efecto de las tecnologías de IA en relación con la privacidad y los derechos humanos, es una buena forma de garantizar la evaluación constante del impacto de la vigilancia y de incluir a la sociedad civil y a los actores externos en el proceso de revisión[62]. **Es preciso que los Gobiernos y los actores de la sociedad civil colaboren entre sí como partes interesadas igualitarias.** Los expertos, académicos e investigadores externos deben ser incorporados al proceso normativo en lugar de pedírseles que, en la instancia final, presenten sus comentarios sobre la idoneidad de proyectos o políticas inminentes[63].

Es necesario un organismo multipartito creado específicamente para tratar cuestiones de vigilancia

La ausencia de un organismo normativo multipartito responsable de atender asuntos de vigilancia, incluida la habilitada por IA, representa un vacío sustancial. Si bien cada vez hay más instituciones que analizan temas de gobernanza de estas tecnologías, como el Observatorio de Políticas en materia de IA de la OCDE o el Instituto para la Inteligencia Artificial Centrada en el Ser Humano de la Universidad de Stanford, no se dedican específicamente a cuestiones de vigilancia. Otras organizaciones de derechos humanos y digitales, como el ACNUDH o la Coalición para la Libertad de Expresión en Internet, han convocado foros que tratan temáticas de vigilancia con IA, aunque en general sus enfoques responden a las circunstancias particulares de cada caso.

La ausencia de un organismo normativo multipartito responsable de atender asuntos de vigilancia, incluida la habilitada por IA, representa un vacío sustancial.

Es necesario contar con un organismo multipartito de carácter permanente encargado de abordar diversas cuestiones de vigilancia. Se dedicaría a aspectos que van desde la elaboración de **normas de uso responsable** hasta el patrocinio de **investigaciones sobre usos emergentes** de nuevas tecnologías, así como a la concepción de **marcos jurídicos** que logren un equilibrio entre el interés público y el perjuicio individual. Aunque dicho organismo podría vincularse con entidades multipartitas existentes, como el Foro para la Gobernanza de Internet o la Asociación Internacional de Inteligencia Artificial, debería incorporar un mandato exclusivo en materia de vigilancia.

Los objetivos de la organización incluirían nuevos enfoques para la prevención de aplicaciones perjudiciales (como los programas informáticos de identificación étnica y de reconocimiento de emociones), la promoción del uso responsable por empresas privadas y Gobiernos, el fomento del intercambio de conocimientos, la incentivación proactiva de cambios de políticas concretas y la generación de conciencia pública sobre asuntos de vigilancia.

La organización debería hacer hincapié en la **promoción de nuevas coaliciones**, como reuniones entre activistas de derechos digitales e ingenieros informáticos, dirigidas a evitar problemas durante la fase de

diseño en lugar de abordarlos una vez que los productos ya se encuentran en el mercado. En cierta medida algunas organizaciones nos ofrecen un modelo parcial: tal es el caso de la Iniciativa de Red Global, que convoca tanto a partes interesadas del sector privado como a defensores de los derechos digitales para debatir inquietudes relativas a la libertad de expresión y a la privacidad. No obstante, la nueva organización se centraría específicamente en cuestiones de vigilancia e incorporaría a su labor un aspecto aplicado, yendo más allá de las interacciones en materia de políticas a fin de debatir características de diseño de productos reales.

Si bien es importante solicitar la intervención de las partes interesadas del ámbito privado, gubernamental y de la sociedad civil, la multiparticipación no debería representar una dilución. **Es preciso que los Gobiernos y empresas que participan en esta iniciativa acrediten una sólida trayectoria en materia de usos y prácticas de vigilancia.** (En consecuencia, no podrían participar los Gobiernos de Egipto o Pakistán, por ejemplo, o las firmas como NSO Group o Clearview AI). El peor de los casos sería que esta organización sufra las mismas patologías que la Unión Internacional de Telecomunicaciones (UIT) o el Consejo de Derechos Humanos de las Naciones Unidas, donde las autocracias con pésimos historiales de derechos humanos son sistemáticamente elegidas para integrarlos u ocupan puestos de dirigencia[64].

El desafío para las democracias

Las democracias deben proceder con mayor vigor en la consideración detallada de las formas de aplicación de sus principios a la gobernanza de la inteligencia artificial, con un seguimiento sostenido en el ámbito interno y una definición de normas internacionales en la materia. Beijín avanza aceleradamente en la formulación de normativa regulatoria de los sistemas de IA. Matt Sheehan, del Fondo Carnegie, señala que los nuevos enfoques para la gobernanza de la IA que están surgiendo en la RPC abordan todos los aspectos, desde reglas para algoritmos en línea hasta principios éticos. También sostiene que las posibles repercusiones reglamentarias se extienden mucho más allá de las fronteras del país: "China realizará algunos de los experimentos regulatorios más grandes del mundo sobre temas que los reguladores europeos han estado debatiendo durante mucho tiempo. La capacidad de las empresas chinas de cumplir con estas nuevas demandas podría ser la base de debates análogos en Europa"[65]. **Mediante estas acciones Beijín logrará una influencia considerable para moldear normas internacionales aplicables a la tecnología de vigilancia con IA, lo que a su vez podría menoscabar la función de la normativa de derechos humanos** en estos marcos. Sin embargo, la RPC no está sola. Los reguladores europeos también han estado ocupados. La Ley de Inteligencia Artificial de la Unión Europea y la Comisión de Inteligencia Artificial del Consejo de Europa ofrecen posibles caminos para que las democracias contrarresten el embate regulatorio de Beijín.

Beijín avanza aceleradamente en la formulación de normativa regulatoria de los sistemas de IA.

La facilitación de una mayor participación pública en la toma de decisiones sobre sistemas de IA es de importancia capital. Mariano-Florentino Cuéllar y Aziz Z. Huq proponen la búsqueda de estrategias para que una más amplia variedad de ciudadanos "logre una mejor comprensión de las alternativas morales y políticas incorporadas en los códigos y en las opciones de diseño de los sistemas de IA"[66]. Estos autores sostienen que es esencial empoderar a la mayor cantidad de usuarios posible "para que influyan e incluso cambien las políticas y los valores de esos sistemas, ya adoptados en la esfera pública o en la privada"[67]. **Es menos importante que la ciudadanía comprenda los mecanismos de funcionamiento de los sistemas específicos de IA, aunque resulta esencial que sea capaz de evaluar sus efectos.** (El tecnólogo David Weinberger explica esta diferencia como una priorización de la "optimización por sobre la explicación")[68]. En este sentido, la sociedad civil puede ayudar a guiar la comprensión, el empoderamiento y la participación del ciudadano en lo relativo a la incidencia social de la IA.

Para dar respuesta al desafío de la vigilancia con IA es necesario que las democracias lleven a cabo diversas tareas importantes en forma simultánea. En primer lugar, deben definir normas regulatorias para guiar el uso responsable de la IA, ya sea por vía de estrategias y leyes nacionales o mediante iniciativas regionales. A fin de garantizar que esta configuración normativa tenga lugar en forma democrática y refleje las inquietudes de los grupos afectados, **es preciso que la ciudadanía cuente con mayores oportunidades** de participar en los procesos deliberativos. Por último, **los Gobiernos democráticos deben formar coaliciones** de Estados con ideas afines para promover valores digitales compartidos. Esta combinación de estrategias permitirá que las democracias se prepararen para promulgar normas internacionales que incorporen la IA a las salvaguardas de derechos humanos y del estado de derecho, pongan coto a los abusos y contrarresten las ambiciones autoritarias de determinar las reglas del juego.

SUPERAR LOS OBSTÁCULOS PARA LA INVESTIGACIÓN SOBRE VIGILANCIA: LECCIONES PARA LA SOCIEDAD CIVIL

// **EDUARDO FERREYRA,** LÍDER DE PROYECTO, ASOCIACIÓN POR LOS DERECHOS CIVILES

La implementación de sistemas de vigilancia con IA suele carecer de transparencia, y las organizaciones de la sociedad civil (OSC) que los investigan necesitan estrategias creativas para superar las maniobras evasivas de proveedores y funcionarios. Mediante acciones de investigación, litigios de interés público y campañas de promoción de causas la Asociación por los Derechos Civiles (ADC)[69] trabaja para contrarrestar usos poco nítidos y no regulados de dichos sistemas en espacios públicos de la Argentina. Eduardo Ferreyra, líder de proyecto de la ADC, ofrece un análisis de las experiencias obtenidas a partir de esas actividades para las OSC que buscan arrojar luz sobre la expansión de la vigilancia digital que opera con inteligencia artificial[70].

Las OSC enfrentan muchos obstáculos comunes en sus procesos de investigación de las tecnologías de vigilancia. En primer lugar, **la información sobre la naturaleza y el alcance de los sistemas de vigilancia no se encuentra fácilmente disponible a través de los canales públicos.** Los Gobiernos nacionales y locales no publican información detallada sobre sus acuerdos

con proveedores. Muy pocas de las solicitudes de acceso a la información presentadas por la ADC tuvieron éxito. En algunos casos las autoridades locales invocaron motivos de secreto comercial o de seguridad pública para rechazarlas; en otros no se proporcionó respuesta alguna. Si bien la Argentina cuenta con una ley de acceso a la información pública con sanciones en caso de incumplimiento, los procesos judiciales son demasiado lentos para brindar un recurso efectivo.

También intentamos contactar a los proveedores privados que suministran dispositivos de vigilancia a funcionarios argentinos. No obstante, en la mayoría de los casos no logramos abrir líneas directas de comunicación con los representantes de esas empresas. Aunque enviamos correos electrónicos a las pocas direcciones que pudimos encontrar en línea, no recibimos respuesta. Como las **empresas multinacionales** que fabrican sistemas de vigilancia tienen su sede fuera de la Argentina, hay **pocas oportunidades para hacer que rindan cuentas**. Asimismo, los funcionarios suelen adquirir los sistemas de vigilancia a través de proveedores locales en lugar de recurrir directamente a los fabricantes. Esta práctica permite que los fabricantes escapen al escrutinio, al no transparentar el papel que desempeñan[71].

Dado que ni los proveedores ni los funcionarios estaban dispuestos a interactuar con nosotros directamente, debimos recurrir a estrategias alternativas. Las declaraciones oficiales sirvieron como punto de partida. Por ejemplo, algunos sistemas de vigilancia fueron lanzados públicamente por los Gobiernos. Asimismo, notamos que había empresas que usaban los despliegues de sistemas de vigilancia como casos de estudio de mercadotecnia que colocaban en sus sitios web. Por ejemplo NEC, la empresa japonesa de TI, presentó las tecnologías de CCTV, de reconocimiento de patentes vehiculares y de reconocimiento facial (TRF) que había suministrado para un programa de vigilancia urbana en la localidad de Tigre, cercana a la ciudad de Buenos Aires[72]. **Los materiales de mercadotecnia dirigidos a otros destinatarios** nos permitieron vislumbrar las relaciones de los proveedores con el sector público local.

Los materiales de mercadotecnia dirigidos a otros destinatarios nos permitieron vislumbrar las relaciones de los proveedores con el sector público local.

Los periodistas independientes también son una fuente esencial de información. Las **investigaciones periodísticas** nos ayudaron a arrojar luz sobre las asociaciones público-privadas detrás de los despliegues de sistemas de vigilancia y sobre el deficiente historial de derechos humanos de las empresas de vigilancia en el mundo. Gracias a OneZero, por ejemplo, nos enteramos de que al parecer la Ciudad de Buenos Aires está utilizando software de reconocimiento facial desarrollado por una firma rusa[73]. Sin embargo, cabe destacar que en general la mayoría de los medios de comunicación argentinos, actuando sin sentido crítico, presentan a las herramientas de vigilancia como la solución para la violencia y el delito.

Estrategias para generar conciencia sobre las tecnologías de vigilancia

Nuestra experiencia nos ha ofrecido numerosas lecciones en lo que hace a la investigación y a la generación de conciencia sobre las tecnologías de vigilancia. A continuación enumeramos algunas de ellas.

1. **Crear coaliciones con otras OSC.** Como los funcionarios públicos y los representantes de las empresas se niegan a dar respuestas, las organizaciones que trabajan en cuestiones de tecnologías de vigilancia deberían estar en contacto entre sí para obtener información, intercambiar contactos y distribuir tareas de investigación. Nuestro estudio de empresas que operan en la Argentina se vio enriquecido por la información suministrada por periodistas y activistas de derechos digitales sobre la conducta de esas corporaciones en otras partes del mundo.
2. **Colaborar estrechamente con periodistas que tengan ideas afines.** Los medios de comunicación independientes pueden ser un gran recurso para arrojar luz sobre acuerdos de vigilancia, aumentar la conciencia pública y alentar el debate mediante el cuestionamiento de mensajes simplistas sobre la tecnología de vigilancia.
3. **Establecer contactos con actores internacionales.** Es posible que, debido a aspectos de imagen pública, los Gobiernos presten más atención a cuestiones de derechos cuando son planteadas por grupos de defensa internacionales o a través de organismos de derechos humanos globales o regionales. Por ejemplo, el Gobierno argentino eliminó información privada de sospechosos menores de edad que constaba en una base de datos pública luego de que Human Rights Watch le enviara una carta al presidente en la que solicitaba ese cambio.[74]
4. **Destacar inquietudes concretas sobre los sistemas de vigilancia.** Las empresas y los políticos promueven los sistemas de vigilancia como respuesta al delito, independientemente de si la evidencia respalda esa perspectiva. Es posible que las comunidades genuinamente preocupadas por la seguridad se inclinen por aceptar ese mensaje. A fin de promover el debate fundamentado sobre la tecnología de vigilancia es necesario que las OSC y los periodistas vayan más allá de las abstracciones y delineen inquietudes inmediatas. Por ejemplo, ¿los datos biométricos recabados por las autoridades presentan vulnerabilidades que permitirán que los cibercriminales le apoderen de ellos?

En los países en desarrollo las investigaciones en materia de vigilancia presentan desafíos. Cuando la opacidad está fuertemente arraigada en la cultura política nacional, las autoridades pueden ver pocos incentivos para ser transparentes. De igual modo, las empresas con sede en el extranjero sienten un muy bajo nivel de presión para revelar información. En vista de estas circunstancias **las OSC deben conducirse en forma colaborativa e inclusiva**. Mediante la estrecha colaboración recíproca, la interacción con periodistas e investigadores y el aprovechamiento de la influencia de la comunidad internacional de derechos humanos pueden llegar a mitigar las asimetrías de poder que ayudan a que Gobiernos y empresas mantengan ocultos los acuerdos de vigilancia.

INICIO DEL DEBATE SOBRE EL RECONOCIMIENTO FACIAL: UN CASO DE ESTUDIO EN BELGRADO

// **DANILO KRIVOKAPIĆ,** DIRECTOR, *SHARE FOUNDATION*

A principios de 2019 funcionarios del Gobierno serbio revelaron planes para la instalación de un sistema de vigilancia de vanguardia que abarcaría toda ciudad de Belgrado, la capital del país, con funcionalidades de reconocimiento de patentes vehiculares y de rostros. Durante los dos años siguientes el grupo de derechos digitales *SHARE Foundation* reformuló el debate sobre este proyecto mediante una iniciativa que movilizó a los activistas tecnológicos, a los residentes locales, a los medios de comunicación y a la comunidad de derechos digitales europea en general. El director de *SHARE Foundation*, Danilo Krivokapi?, presenta el enfoque de la organización.

El anuncio del Ministro del Interior y del Director de la Policía de los planes para instalar **1000 cámaras de alta tecnología de Huawei, el gigante tecnológico de la República Popular China (RPC)**, consolidó las preocupaciones que se venían gestando entre los miembros de nuestro equipo desde que escuchamos por primera vez las propuestas de "actualización" de las cámaras de tránsito de la ciudad. Para el año 2019 los índices mundiales venían registrando un descenso de los derechos civiles en Serbia. La protección institucional estaba

flaqueando y las vulneraciones de los derechos digitales observadas por nuestro equipo nunca fueron abordadas adecuadamente por el sistema judicial. En este contexto los nuevos planes de vigilancia plantearon inquietudes urgentes respecto de las libertades civiles. Con este anuncio, ahora público, nos dispusimos a recabar información más detallada y a aunar nuestras fuerzas en el seno de la comunidad.

El mensaje oficial aseguraba a la ciudadanía que el proyecto le brindaría mayores niveles de seguridad, y que la constante vigilancia automática que implicaba no se utilizaría con fines abusivos[75]. No se reveló ninguna otra información. **El público no recibió información del alcance técnico del sistema, de su precio, de las necesidades específicas que tenía por objeto satisfacer, ni de las salvaguardas necesarias** para mitigar los riesgos potenciales para los derechos humanos. Muchas de nuestras solicitudes sobre el proyecto, presentadas según las normas de libertad de información, fueron rechazadas.

Reformulación del mensaje

No obstante, logramos reconstruir parcialmente el fundamento oficial para la compra estatal de estos sofisticados equipos de vigilancia. En 2009 **Serbia y la RPC celebraron un convenio de cooperación económica y técnica que no fue divulgado**, seguido de otros acuerdos con Huawei en 2014 y en 2017[76]. Este fue el marco **del proyecto "Sociedad Segura"**, destinado a mejorar los sistemas de tecnologías de la información y la comunicación (TIC) y a "aumentar la seguridad de los ciudadanos", según la explicación que nos dio el Ministerio del Interior[77].

Huawei nos proporcionó información adicional sin advertirlo: un caso de estudio publicado en su sitio web brindaba detalles de las características técnicas del proyecto, que además del sistema de cámaras incluía mejoras al "centro de control y datos" del Ministerio del Interior de Serbia, así como una cronología de los acuerdos celebrados entre la empresa y dicha cartera. Al día siguiente de que hiciéramos públicos estos hechos se eliminó del sitio web de Huawei la página con el caso de estudio[78].

Huawei nos proporcionó información adicional sin advertirlo: un caso de estudio publicado en su sitio web brindaba detalles de las características técnicas del proyecto.

En la sociedad profundamente polarizada de Serbia abundan la desinformación y las teorías conspirativas sobre tecnologías digitales. Necesitábamos reformular el mensaje, manteniéndolo simple y sin tonos tecnófobos, y completando los detalles faltantes del proyecto de cámaras. Independientemente de las características valiosas de los beneficios que prometía el sistema de vigilancia, resultaba esencial celebrar un debate abierto e informado sobre la manera en la que esta tecnología podría afectar nuestros derechos individuales y nuestro futuro como sociedad libre.

La ciudadanía había recibido promesas vagas de una solución sofisticada para sus problemas. Ofrecimos una definición más clara de lo que era la tecnología de reconocimiento facial (TRF) y de sus mecanismos de funcionamiento: procesamiento de datos biométricos de manera constante e indiscriminada y recolección de información sobre los rasgos personales e inmutables del sujeto. Si bien aún faltan instrumentos nacionales e internacionales que establezcan parámetros claros para estas prácticas, los grupos de derechos humanos y las autoridades en materia de protección de datos han individualizado una gran cantidad de riesgos de la vigilancia masiva biométrica para la privacidad personal, la igualdad y la no discriminación, las libertades de expresión y de reunión, así como otros derechos humanos que gozan de protección legal[79].

Dada la escasa información oficial disponible, **invitamos al público a que nos ayudara a localizar las ubicaciones físicas de las cámaras inteligentes**. Nuestra iniciativa informal con la etiqueta #hiljadekamera (#MilesdeCámaras) generó rápidamente un mapa, elaborado gracias a la colaboración colectiva, que mostraba las ubicaciones verificadas de las cámaras y sus características técnicas[80]. El cuadro presentado prácticamente no coincidía con el modesto listado oficial de ubicaciones emitido por la policía.

Nuestra iniciativa informal con la etiqueta #hiljadekamera (#MilesdeCámaras) generó rápidamente un mapa, elaborado gracias a la colaboración colectiva, que mostraba las ubicaciones verificadas de las cámaras y sus características técnicas.

Además de estas acciones instrumentamos distintas tácticas concienciación en internet y en espacios físicos. **Se colocaron en los postes de las cámaras** adhesivos vistosos con códigos QR que dirigían a la persona a nuestro sitio web; aparecieron en toda la ciudad **instalaciones artísticas inspiradas en temáticas de vigilancia**; se popularizaron **prendas de calle con la etiqueta #hiljadekamera** (#MilesdeCámaras) a través de una campaña de microfinanciación colectiva, y hubo **micro sitios web**, cortometrajes **documentales** en video y **pódcasts** sobre el tema que recibieron gran atención en línea. También compartimos nuestros resultados con las organizaciones serbias de derechos humanos más tradicionales y utilizamos nuestras redes internacionales de activistas de la privacidad, expertos en tecnología y defensores de derechos digitales para difundir el mensaje a toda Europa.

Puesto que cuando emprendimos esta tarea Serbia se hallaba sujeta a fuertes restricciones por el COVID-19, fue difícil medir el alcance de nuestro mensaje. Cuando publicamos un pedido de colaboración colectiva para reunir fondos adicionales para la campaña los resultados nos dejaron perplejos: superamos nuestra meta inicial en menos de una semana.

A fines del tercer trimestre de 2021 el debate sobre la vigilancia biométrica en Serbia pasó al nivel legislativo. **Descubrimos que el Ministerio del Interior había abierto un debate "público" casi inadvertido sobre la propuesta de una nueva ley de policía, que estaba a punto de cerrarse**. La mencionada propuesta habría introducido fundamentos jurídicos para la vigilancia biométrica masiva. Tras tomar conocimiento de esta iniciativa logramos reacciones de miembros del Parlamento Europeo y de organizaciones de derechos humanos regionales e internacionales. Los medios locales le dedicaron una cobertura extensa al asunto. **En dos días se retiró la propuesta objetada**[81].

Esta lucha está muy lejos de su conclusión. Los sabemos, lo saben los Gobiernos locales, y lo sabe la industria internacional de sistemas de vigilancia. Si bien la transformación digital de la seguridad pública es una parte inevitable del futuro, los ciudadanos, los defensores de derechos humanos y el poder de la participación cívica deben asegurar que la digitalización no conduzca a una distopía.

APÉNDICE 1

TABLA

Estados pendulares y vigilancia con IA

País	Región*	Índice de la democracia electoral (V-Dem)	Tipo de régimen (V-Dem)	Índice de represión digital**	¿Posee capacidades de vigilancia con IA	¿Es miembro de la Iniciativa de la Franja y la Ruta?
Jamaica	WH	0.81	Democracia electoral	-0.95	✓	✓
Czech Republic	EUR	0.81	Democracia electoral	-1.10	✓	✓
Romania	EUR	0.78	Democracia electoral	-0.94	✓	✓
Peru	WH	0.76	Democracia electoral	-1.03	✓	✓
Croatia	EUR	0.75	Democracia electoral	-0.94	✓	✓
Panama	WH	0.75	Democracia electoral	-0.89	✓	✓
Armenia	EUR	0.74	Democracia electoral	-0.57	✓	✓
Israel	MENA	0.74	Democracia liberal	-0.15	✓	
Moldova	EUR	0.74	Democracia electoral	-0.69	✓	✓
South Africa	AFR	0.72	Democracia electoral	-0.59	✓	✓
Senegal	AFR	0.71	Democracia electoral	-0.06		✓
Slovenia	EUR	0.70	Democracia electoral	-0.95	✓	✓
Dominican Republic	WH	0.68	Democracia electoral	-1.25	✓	
Ghana	AFR	0.66	Democracia electoral	-0.35	✓	✓
Brazil	WH	0.66	Democracia electoral	0.06	✓	
Bulgaria	EUR	0.66	Democracia electoral	-0.85		✓
Georgia	EUR	0.65	Democracia electoral	-0.54	✓	✓
Colombia	WH	0.65	Democracia electoral	1.09	✓	
Ecuador	WH	0.64	Democracia electoral	0.47	✓	✓
Namibia	AFR	0.63	Democracia electoral	-0.39	✓	✓
Mexico	WH	0.63	Democracia electoral	-0.44	✓	
Mongolia	EAP	0.63	Democracia electoral	-0.87	✓	✓
Liberia	AFR	0.62	Democracia electoral	0.18		✓
Lesotho	AFR	0.62	Democracia electoral	0.06		✓
Malawi	AFR	0.62	Democracia electoral	-0.08		

Continuará

País	Región*	Índice de la democracia electoral (V-Dem)	Tipo de régimen (V-Dem)	Índice de represión digital**	¿Posee capacidades de vigilancia con IA	¿Es miembro de la Iniciativa de la Franja y la Ruta?
Kosovo	EUR	0.60	Democracia electoral	-0.38		
Botswana	AFR	0.59	Democracia liberal	-0.67	✓	
Nepal	SCA	0.59	Democracia electoral	0.58		✓
North Macedonia	EUR	0.59	Democracia electoral	-0.35		✓
Indonesia	EAP	0.59	Democracia electoral	0.03	✓	✓
Poland	EUR	0.59	Democracia electoral	-0.63	✓	✓
Sri Lanka	SCA	0.57	Democracia electoral	0.50	✓	✓
Paraguay	WH	0.57	Democracia electoral	-0.73	✓	
Tunisia	MENA	0.56	Autocracia electoral	-0.44	✓	✓
Sierra Leone	AFR	0.55	Democracia electoral	0.09		✓
Bosnia and Herzegovina	EUR	0.53	Democracia electoral	-0.50	✓	✓
Niger	AFR	0.52	Democracia electoral	0.49		✓
Ukraine	EUR	0.52	Democracia electoral	0.32	✓	✓
Guatemala	WH	0.50	Democracia electoral	-0.48		
The Gambia	AFR	0.50	Autocracia electoral	-0.15		✓
Montenegro	EUR	0.50	Autocracia electoral	-0.35		✓
Nigeria	AFR	0.49	Autocracia electoral	0.11	✓	✓
Madagascar	AFR	0.48	Autocracia electoral	0.16	✓	✓
Albania	EUR	0.48	Autocracia electoral	-0.19		✓
Kenya	AFR	0.47	Autocracia electoral	0.00	✓	✓
El Salvador	WH	0.47	Autocracia electoral	-0.27		✓
Hungary	EUR	0.46	Autocracia electoral	-0.45	✓	✓
Lebanon	MENA	0.46	Autocracia electoral	0.98	✓	✓
India	SCA	0.44	Autocracia electoral	0.97	✓	
Ivory Coast	AFR	0.43	Autocracia electoral	0.20	✓	✓
Philippines	EAP	0.43	Autocracia electoral	0.64	✓	✓
Papua New Guinea	EAP	0.42	Autocracia electoral	-0.30	✓	✓
Benin	AFR	0.42	Autocracia electoral	-0.02		✓
Kyrgyzstan	SCA	0.42	Autocracia electoral	0.02	✓	✓
Malaysia	EAP	0.41	Autocracia electoral	0.03	✓	✓

Continuará

País	Región*	Índice de la democracia electoral (V-Dem)	Tipo de régimen (V-Dem)	Índice de represión digital**	¿Posee capacidades de vigilancia con IA	¿Es miembro de la Iniciativa de la Franja y la Ruta?
Singapore	EAP	0.40	Autocracia electoral	0.31	✓	✓
Honduras	WH	0.39	Autocracia electoral	-0.16		
Mauritania	AFR	0.39	Autocracia electoral	0.33		✓
Gabon	AFR	0.38	Autocracia electoral	0.76		✓
Iraq	MENA	0.37	Autocracia electoral	0.78	✓	✓
Togo	AFR	0.37	Autocracia electoral	0.54		✓
Pakistan	SCA	0.36	Autocracia electoral	0.65	✓	✓
Tanzania	AFR	0.36	Autocracia electoral	0.38		✓
Democratic Republic of the Congo	AFR	0.36	Autocracia electoral	0.28		✓
Mozambique	AFR	0.36	Autocracia electoral	-0.13		✓
Angola	AFR	0.35	Autocracia electoral	0.02	✓	✓
Serbia	EUR	0.34	Autocracia electoral	0.11	✓	✓

*Abreviaciones regionales: WH = Western Hemisphere; EUR = Europe and Eurasia; AFR = Sub Saharan Africa; MENA = Middle East and North Africa; SCA = South and Central Asia; and EAP = East Asia and Pacific

**En cuanto al índice de represión digital, consúltese *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*, de Steven Feldstein; datos actualizados a 2021. Mendeley Data, V3, 2022, doi: 10.17632/5dnfmtgbfs.3

NOTAS

La lucha global ante la vigilancia con IA

1 Steven Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*, (New York: Oxford University Press, 2021), 218.

2 Para más información, véase: Maya Wang, *China's Algorithms of Repression*, Human Rights Watch, 1 mayo 2019, www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

3 Para más información sobre los riesgos que supone la IA para los derechos humanos, véase: *Privacy and Free Expression in the Age of Artificial Intelligence,* abril 2018, www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf.

4 Para más información, véase: LeRoy Ashby and Rod Gramer, *Fighting the Odds: The Life of Senator Frank Church,* (Pullman, Washington: Washington State University Press, 1994), 478.

5 Morgan Meaker, "Marseille's Fight against AI Surveillance," Coda Story, 26 marzo 2020, https://www.codastory.com/authoritarian-tech/ai-surveillance-france-crime/; y Auriane Dirou, "The French Global Security Law: Security or Liberties?," *Just Security,* 15 abril 2021, https://justsecurity.org/75754/the-french-global-security-law-security-or-liberties/.

6 "Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks," Government Accountability Office, 29 junio 2021, www.gao.gov/products/gao-21-518; y Ryan Mac et al., "Surveillance Nation," *BuzzFeed News*, 6 abril 2021, www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition.

7 James Vincent, "FBI Used Facial Recognition to Identify a Capitol Rioter from His Girlfriend's Instagram Posts," Verge, 21 abril 2021, www.theverge.com/2021/4/21/22395323/fbi-facial-recognition-us-capital-riots-tracked-down-suspect.

8 Elizabeth Dworkin, "Israel escalates surveillance of Palestinians with facial recognition program in West Bank," *Washington Post,* 8 noviembre 2021, www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html.

9 Vanessa A. Boese et al., "Autocratization Changing Nature? Democracy Report 2022," Varieties of Democracy Institute (V-Dem), 2022, https://v-dem.net/media/publications/dr_2022.pdf.

10 Prabhjote Gill, "India Is Ramping Up the Use of Facial Recognition to Track Down Individuals Without Any Laws to Keep Track of How This Technology Is Being Used," *Business Insider India,* 10 febrero 2021, www.businessinsider.in/tech/news/what-is-facial-recognition-technology-and-how-india-is-using-it-to-track-down-protestors-and-individuals/articleshow/80782606.cms.

11 Bojan Stojkovski, "Big Brother Comes to Belgrade," *Foreign Policy*, 18 junio 2019, https://foreignpolicy.com/2019/06/18/big-brother-comes-to-belgrade-huawei-china-facial-recognition-vucic/.

12 Umer Ali and Ramsha Jahangir, "Pakistan Moves to Install Nationwide 'Web Monitoring System,'" Coda Story, 24 octubre 2019, www.codastory.com/authoritarian-tech/surveillance/pakistan-nationwide-web-monitoring/.

13 Daniel Zhang et al., "The AI Index 2021 Annual Report," AI Index Steering Committee, Human-Centered AI Institute, Stanford University, marzo 2022, https://aiindex.stanford.edu/wp-content/uploads/2021/11/2021-AI-Index-Report_Master.pdf.

14 Steven Feldstein, *The Global Expansion of AI Surveillance,* Carnegie Endowment for International Peace, 17 septiembre 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

15 Steven Feldstein, "AI & Big Data Global Surveillance Index (2022 updated)," Mendeley Data, V3, 2022, https://data.mendeley.com/datasets/gjhf5y4xjp/3.

16 Las clasificación de sistemas políticos utiliza la medida "regímenes del mundo" de V-Dem. Para más información, véase: Lührmann et al., "V-Dem Codebook v11.1," Varieties of Democracy (V-Dem) Project, 2021, www.v-dem.net/static/website/img/refs/codebookv111.pdf.

17 *Mapping China's Digital Silk Road,* Center for Strategic and International Studies, Reconnecting Asia Project, 19 octubre 2021, https://reconasia.csis.org/mapping-chinas-digital-silk-road/.

18 Sheena Chestnut Greitens, "China's Surveillance State at Home & Abroad: Challenges for U.S. Policy," Working Paper for the Penn Project on the Future of U.S.-China Relations, 2020, https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b/732/files/2020/10/Sheena-Greitens_Chinas-Surveillance-State-at-Home-Abroad_Final.pdf.

19 Jane Wakefield, "AI Emotion-Detection Software Tested on Uyghurs," *BBC News*, 26 mayo 2021, www.bbc.com/news/technology-57101248; "Dahua Provides 'Uyghur Warnings' to China Police," IPVM, 9 febrero 2021, https://ipvm.com/reports/dahua-uyghur-warning; y Drew Harwell and Eva Dou, "Huawei Tested AI Software That Could Recognize Uighur Minorities and Alert Police, Report Says," *Washington Post*, 8 diciembre 2020, www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/.

20 "Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights," Article 19, enero 2021, www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf.

21 Dahlia Peterson, *How China Harnesses Data Fusion To Make Sense Of Surveillance Data*, Brookings Institution, 23 septiembre 2021, www.brookings.edu/techstream/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/.

22 De acuerdo con un análisis del Center for Security and Emerging Technology (Centro de Seguridad y Tecnología Emergente) de la Universidad de Georgetown, las instituciones de la RPC son las responsables "de más de un tercio de las publicaciones en investigación tanto de visión artificial como de vigilancia visual". Para más información, véase: Ashwin Acharya, Max Langenkamp, and James Dunham, "Trends in AI Research for the Visual Surveillance of Populations," Center for Security and Emerging Technology, enero 2022, https://doi.org/10.51593/20200097.

23 Cate Cadell, "China Harvests Masses of Data on Western Targets, Documents Show," *Washington Post*, 31 diciembre 2021, www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html.

24 Feldstein, *The Rise of Digital Repression*, 241.

25 *Out of Control: Failing EU Laws for Digital Surveillance Export,* Amnesty International, 21 septiembre 2020, www.amnesty.org/en/documents/eur01/2556/2020/en; and Mara Hvistendahl, "How Oracle Sells Repression in China," Intercept, 18 febrero 2021, https://theintercept.com/2021/02/18/oracle-china-police-surveillance/.

26 Para más información, véase: Steven Feldstein and David Wong, "New Technologies, New Problems—Troubling Surveillance Trends in America," *Just Security,* 6 agosto 2020, www.justsecurity.org/71837/new-technologies-new-problems-troubling-surveillance-trends-in-america/.

27 Describe un ejemplo. Paresh Dave, "Companies Bet on AI Cameras to Track Social Distancing, Limit Liability," *Reuters,* 27 abril 2020, www.reuters.com/article/us-health-coronavirus-surveillance-tech-idUSKCN22914R; Antonia do Carmo Barriga et al., "The COVID-19 Pandemic: Yet Another Catalyst for Governmental Mass Surveillance?" *Social Sciences & Humanities Open* 2, (2020), www.sciencedirect.com/science/article/pii/S2590291120300851; y Melissa Heikkla, "Politico AI: Decodes: Color-blind Policy—France Debates Facial Recognition—MEPs AI Law Wishlist," *Politico*, 17 marzo 2021, www.politico.eu/newsletter/ai-decoded/politico-ai-decoded-color-blind-policy-france-debates-facial-recognition-meps-ai-law-wishlist/.

28 Wim Naudé, "Artificial Intelligence vs COVID-19: Limitations, Constraints and Pitfalls," *AI & SOCIETY* 35 (1 septiembre 2020): 761–65, https://doi.org/10.1007/s00146-020-00978-0; y para más información, véase "The Role of AI Technology in Pandemic Response and Preparedness: Recommended Investments and Initiatives," National Security Commission on Artificial Intelligence, 25 junio 2020, www.nscai.gov/wp-content/uploads/2021/01/NSCAI_White-Paper_The-Role-of-AI-Technology-in-Pandemic-Response-and-Preparedness.pdf.

29 Chris Buckley, Vivian Wang, and Keith Bradsher, "Living by the Code: In China, Covid-Era Controls May Outlast the Virus," *New York Times,* 30 enero 2022, www.nytimes.com/2022/01/30/world/asia/covid-restrictions-china-lockdown.html.

30 Darren Bylar, "The Covid Tech That Is Intimately Tied to China's Surveillance State," *MIT Tech Review,* 11 octubre 2021, www.technologyreview.com/2021/10/11/1036582/darren-byler-xinjiang-china-uyghur-surveillance.

31 Para más información, véase: Robert Morgus, Jocelyn Woolbright, and Justin Sherman, *The Digital Deciders*, New America, 23 octubre 2018, www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/.

32 El informe utilizó la siguiente metodología para identificar a los estados pendulares. Se filtró el índice de democracia electoral de V-Dem para incluir a todos los países con un puntaje entre Serbia (0,342) y Jamaica (0,81). Luego se redujo el listado con la eliminación de pequeños países insulares y estados con poblaciones por debajo de 2 millones de habitantes. Los países con claras características autoritarias y/o los Estados recientemente asediados por tumultos e inestabilidad también quedaron excluidos (Afganistán, Burkina Faso, República Centroafricana, Guinea Bissau, Haití, Mali, Myanmar, Somalilandia). En virtud de este método, el listado de estados pendulares incluye 67 países.

33 Feldstein, *The Rise of Digital Repression.*

34 Distintos investigadores, como Sheena Chestnut Greitens, Iginio Gagliardone, Matthew S. Erie y Thomas Streinz, observan que una combinación de "factores de empuje y tracción" explica mejor por qué algunos regímenes adquieren tecnologías de vigilancia de la RPC y cómo los utilizarán. Para más información, véase: Sheena Chestnut Greitens, *Dealing with Demand for China's Global Surveillance Exports,* Brookings Institution, abril 2020, www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/; Iginio Gagliardone, *China, Africa, and the Future of the Internet,* (London: Zed Books, 2019); y Matthew S. Erie and Thomas Streinz, "The Beijing Effect: China's' Digital Silk Road's Transnational Data Governance." *New York University Journal of International Law and Politics* (JILP) 54 (otoño 2021): 1-91, www.nyujilp.org/wp-content/uploads/2022/02/NYUJILP_Vol54.1_Erie_Streinz_1-91.pdf.

35 Akın Ünver, "Motivations for the Adoption and Use of Authoritarian AI Technology," *Issues on the Frontlines of Technology and Politics,* ed. Steven Feldstein (Washington, D.C.: Carnegie Endowment for International Peace, 19 octubre 2021), 16, https://carnegieendowment.org/2021/10/19/motivations-for-adoption-and-use-of-authoritarian-ai-technology-pub-85510; y por favor véalo: Akın Ünver and Arhan S. Ertan, "Politics of Artificial Intelligence Adoption: Unpacking the Regime Type Debate," *Democratic Frontiers: Algorithms and Society,* ed. Michael Filimowicz (New York: Routledge, 2022).

36 *Nigeria: Freedom on the Net 2021 Country Report*, Freedom House, last modified 20 September 2021, https://freedomhouse.org/country/nigeria/freedom-net/2021; y *Singapore: Freedom on the Net 2021 Country Report,* Freedom House, última modificación 20 septiembre 2021, https://freedomhouse.org/country/singapore/freedom-net/2021.

37 Gautam Bhatia, "India's Growing Surveillance State," *Foreign Affairs,* 19 febrero 2020, www.foreignaffairs.com/articles/india/2020-02-19/indias-growing-surveillance-state.

38 Sangeeta Mahapatra, *Digital Surveillance and the Threat to Civil Liberties in India,* German Institute for Global and Area Studies, 2021, www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india.

39 Sheridan Prasso, "Huawei's Claims That It Makes Cities Safer Mostly Look Like Hype," *Bloomberg,* 12 noviembre 2019, www.bloomberg.com/news/articles/2019-11-12/huawei-s-surveillance-network-claims-face-scrutiny?sref=QmOxnLFz.

40 Carey Baraka, "The Failed Promise of Kenya's Smart City," *Rest of World,* 1 junio 2021, https://restofworld.org/2021/the-failed-promise-of-kenyas-smart-city/.

41 Feldstein, *The Rise of Digital Repression,* 165.

42 Sheena Chestnut Greitens, *Dealing with Demand for China's Global Surveillance Exports.*

43 Ben Wagner, "Ethics As an Escape from Regulation: From "Ethics-Washing" to Ethics-Shopping?" *Being Profiled: Cogitas Ergo Sum,* eds. Emre Bayamlıoğlu, Irina Baraliuc, Liisa Janssens, and Mireille Hildebrandt, (Amsterdam: Amsterdam University Press, 2018), acceda en línea aquí por favor: www.cohubicol.com/assets/uploads/being-profiled-16-wagner.pdf; y Eileen Donahoe and Megan MacDuffee Metzger, "Artificial Intelligence and Human Rights," *Journal of Democracy* (abril 2019): 115–26, www.journalofdemocracy.org/articles/artificial-intelligence-and-human-rights/.

44 *"Artificial Intelligence Act," European Parliament, 2021,* https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en.

45 "CAHAI—Ad hoc Committee on Artificial Intelligence," Council of Europe, 2021, www.coe.int/en/web/artificial-intelligence/cahai.

46 "Artificial Intelligence risks to privacy demand urgent action—Bachelet," United Nations Human Rights Office of the High Commissioner, 15 septiembre 2021, www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet.

47 "Resolution on the Right to Privacy in the Digital Age," (A/HRC/48/L.9/REV.1), United Nations Human Rights Council, 48th session, 13 septiembre-8 octubre 2021, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G21/274/69/PDF/G2127469.pdf?OpenElement.

48 "Draft Text of the Recommendation on the Ethics of Artificial Intelligence," United Nations Educational, Scientific and Cultural Organization, 25 junio 2021, https://unesdoc.unesco.org/ark:/48223/pf0000377897.

49 Rachel Metz, "Portland Passes Broadest Facial Recognition Ban in the US," CNN, 10 septiembre 2020, https://edition.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html.

50 "ICYMI: WIRED (Opinion): Americans Need a Bill of Rights for an AI-Powered World," White House, 22 octubre 2021, www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/.

51 "Treasury Identifies Eight Chinese Tech Firms as Part of The Chinese Military-Industrial Complex," U.S. Department of Treasury, 16 diciembre 2021, https://home.treasury.gov/news/press-releases/jy0538; y James Vincent, "US announces AI software export restrictions," Verge, 5 enero 2020, www.theverge.com/2020/1/5/21050508/us-export-ban-ai-software-china-geospatial-analysis.

52 Charles Bradley and Richard Wingfield, "National Artificial Intelligence Strategies and Human Rights: A Review," 2nd ed., Global Partners Digital and Stanford's Global Digital Policy Incubator, abril 2021, www.gp-digital.org/wp-content/uploads/2021/05/NAS-and-human-rights_2nd_ed.pdf.

53 Un análisis similar de 34 países con planes de IA que llevó a cabo Fatima et al., concluyó que "la mayoría de los planes no contenía ninguna información sobre las estrategias de implementación o los mecanismos de rastreo concretos, lo que deja al descubierto la naturaleza mayormente aspiracional de los planes". Los planes se enfocaban en su mayor parte en cómo los Gobiernos deberían aprovechar la IA para modernizar el sector público, y cómo se puede beneficiar la industria para mejorar su competitividad. Para más información, véase: Samar Fatima, Kevin C. Desouza, y Gregory S. Dawson, "National Strategic Artificial Intelligence Plans: A Multi-Dimensional Analysis," *Economic Analysis and Policy* 67 (2020): 178-194, www.sciencedirect.com/science/article/abs/pii/S0313592620304021.

54 Niharika Mandhana, "Huawei's Video Surveillance Business Hits Snag in Philippines," *Wall Street Journal,* 20 febrero 2019, www.wsj.com/articles/huaweis-video-surveillance-business-hits-snag-in-philippines-11550683135.

55 Elias Biryabarema, "Ugandan Opposition, Activists Denounce Digital Car Tracker Plan," *Reuters,* 19 julio 2021, www.reuters.com/world/africa/ugandan-opposition-activists-denounce-digital-car-tracker-plan-2021-07-29/.

56 Ryan Gallagher, "Francisco-Backed Sandvine Nixes Belarus Deal," *Bloomberg,* 15 septiembre 2020, www.bloomberg.com/news/articles/2020-09-15/sandvine-says-it-will-no-longer-sell-its-products-in-belarus.

57 Justin Sherman, "Data Brokers and Sensitive Data on U.S. Individuals," Duke University Sanford Cyber Policy Program, 2021, 9, https://sites.sanford.duke.edu/techpolicy/wp-content/uploads/sites/17/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

58 Sherman, "Data Brokers and Sensitive Data," 12.

59 "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework," United Nations Human Rights Office of the High Commissioner (UN OHCHR), (HR/PUB/11/04), 2011, www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

60 "Guiding Principles," UN OHCHR.

61 "Safeguards for Public-Private Surveillance Partnerships," Privacy International, diciembre 2021, https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships.

62 "Final Report," National Security Commission on Artificial Intelligence, 2021, www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

63 La iniciativa de la Casa Blanca de crear una "declaración de derechos para una sociedad automatizada", por ejemplo, requiere de una gran cantidad de opiniones y aportes externos, incluso mediante la organización de dos sesiones de audiencias públicas y seis eventos públicos para debatir riesgos, beneficios y principios centrales relacionados con la regulación responsable de la tecnología de IA. Para más información, véase: "Join the Effort to Create A Bill of Rights for an Automated Society," White House, 10 noviembre 2021, www.whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/.

64 Mary Hui, "China's election to the UN Human Rights Council revealed its shaky global status," Quartz, 14 octubre 2020, https://qz.com/1917295/china-elected-to-un-rights-council-but-with-lowest-support-ever/.

65 Matt Sheehan, *China's New AI Governance Initiatives Shouldn't Be Ignored,* Carnegie Endowment for International Peace, 4 enero 2022, https://carnegieendowment.org/2022/01/04/china-s-new-ai-governance-initiatives-shouldn-t-be-ignored-pub-86127.

66 Mariano-Florentino Cuéllar and Aziz Z. Huq, *The Democratic Regulation of Artificial Intelligence,* The Knight First Amendment Institute, 31 enero 2022, https://knightcolumbia.org/content/the-democratic-regulation-of-artificial-intelligence.

67 Cuéllar and Huq, *Democratic Regulation.*

68 Weinberger señala: "utilizar los procesos existentes para formulación de políticas —reguladores, legisladores, sistemas judiciales, ciudadanos indignados, políticos que discuten— a fin de decidir para qué queremos optimizar estos sistemas. Medir los resultados. Ajustar los sistemas cuando no logran llegar a las marcas. Celebrar y mejorarlos cuando logran hacerlo." Para más información, véase: David Weinberger, "Optimization over Explanation: Maximizing the Benefits of Machine Learning Without Sacrificing Its Intelligence," *Medium,* 28 enero 2018, https://medium.com/berkman-klein-center/optimization-over-explanation-41ecb135763d.

Superar los obstáculos de la investigación sobre vigilancia: lecciones para la sociedad civil

69 Para más información, visite: https://adc.org.ar/en/home.

70 Este ensayo se basa en investigación publicada en el informe de la ADC, Tecnologías de Vigilancia en Argentina, de diciembre de 2021, escrito por Alejo Kiguel, Eduardo Ferreyra y Leandro Ucciferri (disponible en: https://adc.org.ar/wp-content/uploads/2022/03/ADC-Surveillance-Technology-in-Argentina.pdf) y en Gaspar Pisanu et al., Surveillance Tech in Latin America: Made Abroad, Deployed at Home, Access Now, 10 Agosto 2021, www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf.

71 Pisanu et al., *Surveillance Tech in Latin America,* 7.

72 El sitio archivado está disponible en: "Case Study: Integrated Urban Safety Solutions, Tigre City," NEC, 2016, https://web.archive.org/web/20170321095617/http:/www.nec.com/en/case/tigre/pdf/brochure.pdf (accedido 21 marzo 2017).

73 Dave Gershgorn, "The U.S. Fears Live Facial Recognition. In Buenos Aires, It's a Fact of Life," *OneZero,* 4 marzo 2020, https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d.

74 "Argentina: Child Suspects' Private Data Published Online," Human Rights Watch, 9 octubre 2020, www.hrw.org/news/2020/10/09/argentina-child-suspects-private-data-published-online.

Inicio del debate sobre el reconocimiento facial: un caso de estudio en Belgrado

75 Danijela Vukosavljević, "The Privacy of Citizens Will Not Be Endangered," *Politika,* 7 octubre 2019, https://www-politika-rs.translate.goog/sr/clanak/439334/Privatnost-gradana-nece-biti-ugrozena?_x_tr_sl=sr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc; y "What and When Will 1,000 New Cameras Be Filmed on City Streets," RTS, 9 febrero 2019, https://www-rts-rs.translate.goog/page/stories/sr/story/125/drustvo/3415215/sta-ce-i-koga-snimati-1000-novih-kamera-po-gradskim-ulicama.html?_x_tr_sl=sr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc.

76 Stojkovski, "Big Brother Comes to Belgrade."

77 "MUP Decision," letter published by SHARE Foundation, 7 marzo 2019, https://resursi.sharefoundation.info/wp-content/uploads/2019/03/Resenje-MUP-7.3.2019..pdf.

78 La página archivada está disponible en: https://archive.ph/pZ9HO. Para más información, véase: "Huawei Knows Everything About Cameras in Belgrade—And They Are Glad to Share," SHARE Foundation, 29 marzo 2019, www.sharefoundation.info/en/huawei-knows-everything-about-cameras-in-belgrade-and-they-are-glad-to-share/.

79 Para una breve descripción de los resultados, véase: "Consultation on the proposal for the Zakon o Unutrašnjim Poslovima," published letter from EDRi, SHARE Foundation, 17 septiembre 2021, https://www.sharefoundation.info/wp-content/uploads/EDRi-Civil-Society-consultation-on-the-proposal-for-the-Zakon-o-unutrasnjim-poslovima.pdf.

80 "Hiljade.Kamera.rs: Community Strikes Back against Mass Surveillance," SHARE Foundation, 19 mayo 2020, www.sharefoundation.info/en/hiljade-kamera-rs-community-strikes-back/.

81 "Draft Withdrawal A Step Towards Moratorium on Biometric Surveillance," SHARE Foundation, 23 septiembre 2019, www.sharefoundation.info/en/draft-withdrawal-a-step-towards-moratorium-on-biometric-surveillance/.

LOS COLABORADORES

LOS AUTORES

Steven Feldstein es investigador principal en el Programa sobre Democracia, Conflicto y Gobernanza del Fondo Carnegie, en donde se dedica principalmente a cuestiones de tecnología y democracia, derechos y política exterior estadounidense. Es autor de numerosas publicaciones y ha escrito sobre muchos temas, tales como la forma en la que la inteligencia artificial reconfigura la represión, la geopolítica de la tecnología, el papel de China en el avance del autoritarismo digital y el efecto del COVID-19 en las democracias. También es autor de *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance* (Oxford University Press, 2021). Su perfil en twitter es @SteveJFeldstein.

Eduardo Ferreyra es líder de proyectos en la Asociación por los Derechos Civiles, una organización de la sociedad civil con sede en Buenos Aires, Argentina. Su trabajo se centra en la gestión de proyectos sobre tecnología y derechos humanos. Egresó como Abogado de la Universidad Nacional de Tucumán y cuenta con una Maestría en Derechos Humanos y Democratización en América Latina de la Universidad Nacional de San Martín. Su perfil en twitter es @ferreyraedu.

Danilo Krivokapić es director de la *SHARE Foundation*, una organización de derechos digitales con sede en Belgrado, Serbia. Obtuvo su título en derecho de la Universidad de Belgrado y sus ámbitos de trabajo y conocimiento especializado abarcan la protección de datos, los efectos sobre la privacidad causados por los modelos de negocios basados en datos, las normas jurídicas relativas a la seguridad de la información y el cibercrimen. Es fundador de la iniciativa #hiljadekamera ((#MilesdeCámaras), una comunidad de individuos y organizaciones que promueve el uso responsable de la tecnología de vigilancia. Su perfil en twitter es @dkrivokapic.

LA EDITORA

Beth Kerley es directora de programas de la sección de investigación y conferencias del *International Forum for Democratic Studies* (Foro Internacional de Estudios Democráticos) de la National Endowment for Democracy (Fundación Nacional para la Democracia). Dirige la cartera de tecnologías emergentes del Foro, que abarca los desafíos y las oportunidades para la democracia planteadas por los avances tecnológicos (como el aprendizaje automático, el internet de las cosas y la analítica de macrodatos) para las nuevas herramientas de política y gobernanza. Se desempeñó como editora asociada del *Journal of Democracy*. Posee un Doctorado en Historia de la Universidad de Harvard y una Licenciatura en Servicio Exterior de la Universidad de Georgetown.

AGRADECIMIENTOS

Steven Feldstein desea agradecer a Brian Kot por su ayuda en las tareas de edición e investigación, así como a dos revisores anónimos por sus comentarios tan útiles y valiosos. Los autores también agradecen las contribuciones del personal y dirigentes del Foro, entre ellos Christopher Walker, John Glenn, Kevin Sheives, John Engelken, Rachelle Faust, Lily Sabol y Daniel Cebul, pues el aporte de todos ellos fue esencial para la edición y publicación de este informe. Un agradecimiento especial para Beth Kerley, cuya colaboración y visión para este proyecto fueron fundamentales para concretarlo. El Foro desea agradecer a Factor3 Digital por su trabajo y respaldo invaluables en el diseño de este documento para su publicación.

FOTOGRAFÍAS

Foto de portada: Foto de Trismegist san/Shutterstock

Página 6: Foto de Sergey Nivens/Shutterstock

Página 9: Foto de zmpixes/Shutterstock

Página 12: Foto de Karolis Kavolelis/Shutterstock

Página 16: Foto proporcionada por Danilo Krivokapić de SHARE Foundation

Página 19: Foto proporcionada por Eduardo Ferreyra de ADC

Página 21: Foto de Thierry Monasse/Getty Images

Página 25: Foto de STEKLO/Shutterstock

Página 28: Danilo Krivokapić de SHARE Foundation

Fecha de traducción: noviembre de 2022

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 de 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 becas 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.

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.

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

@thinkdemocracy

ThinkDemocracy