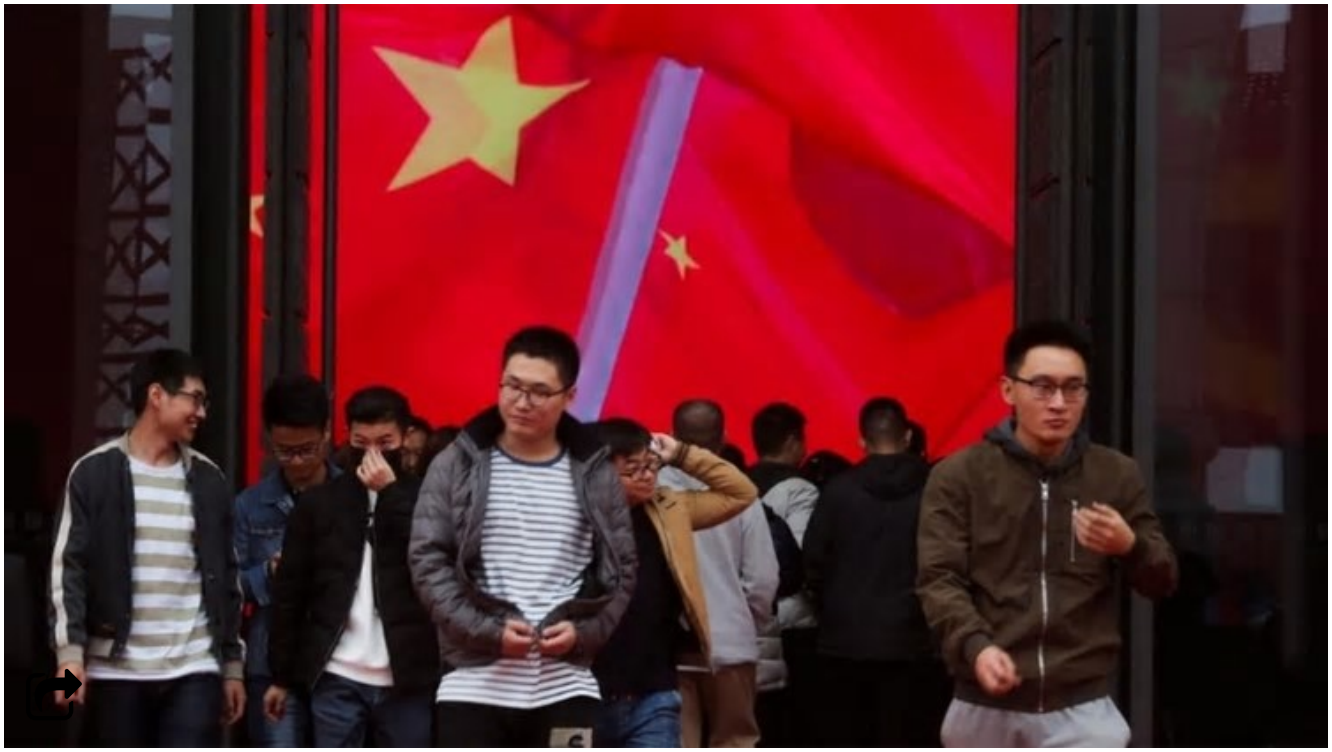
Persecución a opositores y perpetuar regímenes autoritarios, los riesgos detrás de la tecnología china de vigilancia

Por Evan Ellis



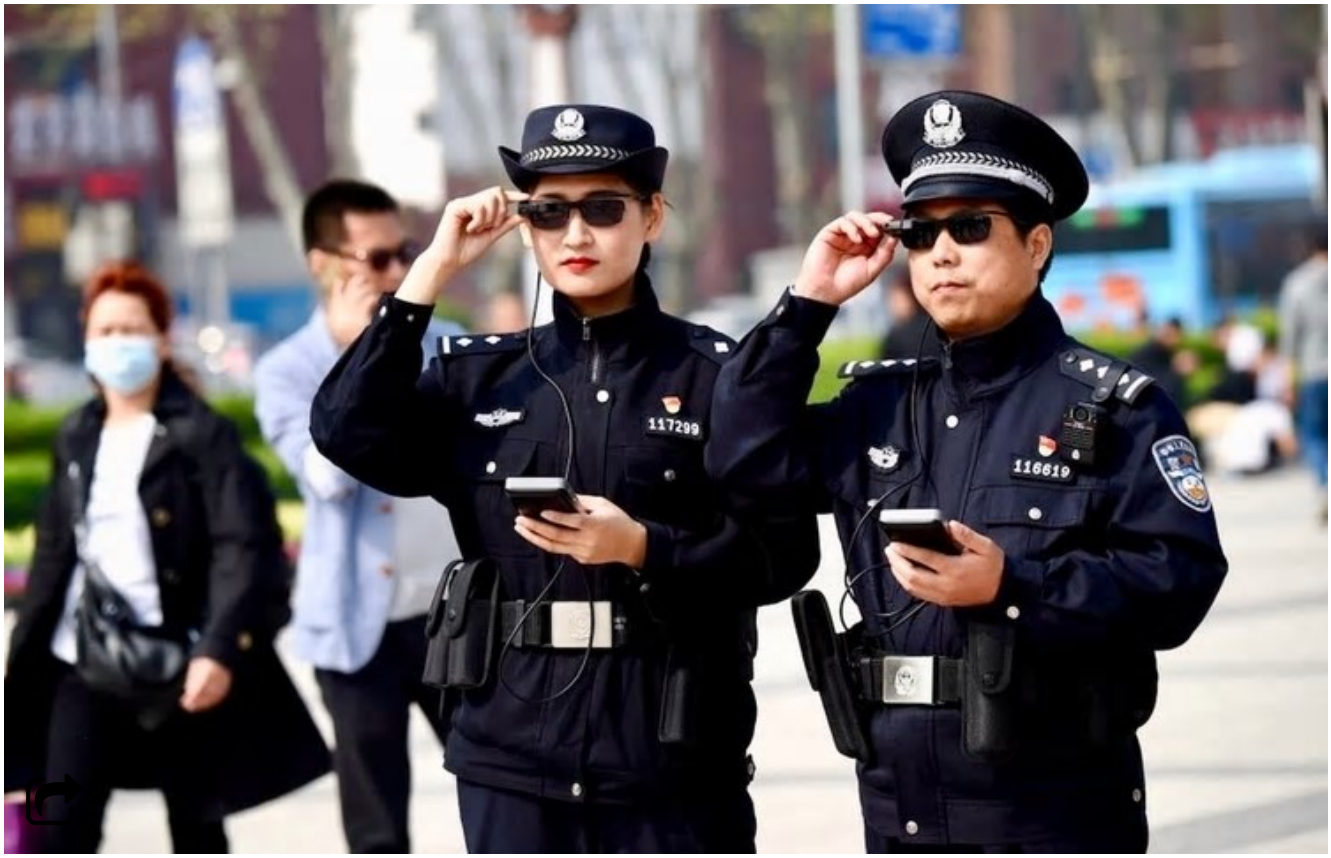
El mismo sistema de vigilancia que aplica a los ciudadanos chinos lo aplicó para América Latina. (Foto: Especial)

En febrero de 2019, en una noticia que pasó casi desapercibida en Washington, la pequeña nación sudamericana de Uruguay comenzó a instalar la primera de 2.100 cámaras de vigilancia, donadas por la República Popular China para mejorar el control de sus fronteras con los vecinos Argentina y Brasil.

La medida destaca la significativa profundización de la relación entre Uruguay y China en la última década, incluido el establecimiento de una "asociación estratégica" en octubre de 2016 y la firma de un memorando de entendimiento en agosto de 2018 para que Uruguay se una a la iniciativa china Iniciativa del Cinturón y Ruta de la Seda. (A pesar de estar tan lejos China como es posible geográficamente).

Más allá de Uruguay, el desarrollo también destaca una dimensión poco discutida pero importante del avance chino: la expansión de sus ventas globales de tecnologías de vigilancia y control. Aunque la prensa y los líderes políticos de los Estados Unidos han prestado gran atención a los riesgos de emplear compañías de telecomunicaciones chinas como Huawei, el tema igualmente serio pero más reciente del crecimiento de las ventas de los sistemas de vigilancia chinos ha sido menos discutido.

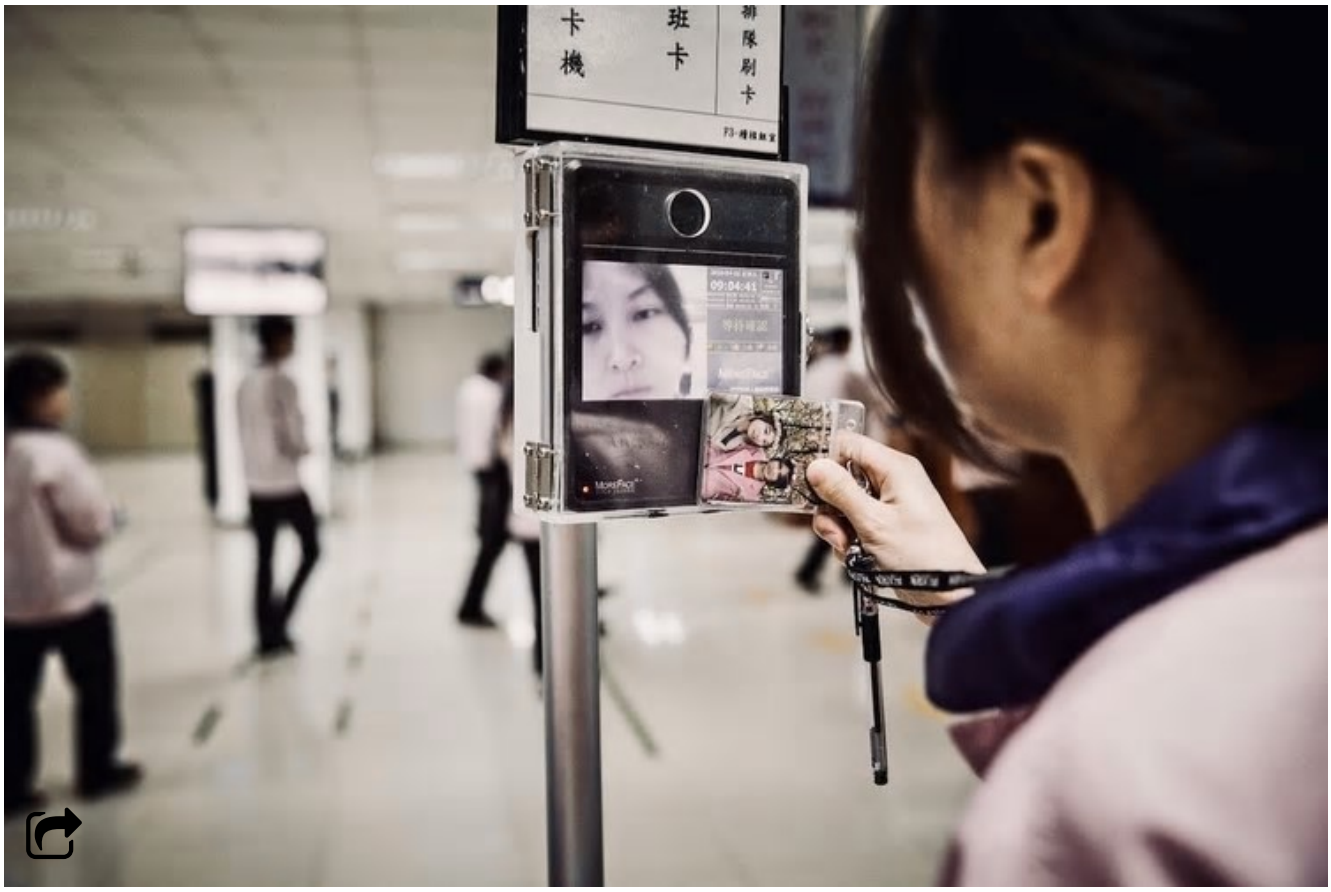
La instalación de sistemas de vigilancia chinos, adquiridos a través de donaciones del gobierno de la República Popular China o contratos comerciales, es un fenómeno creciente en América Latina y en otros lugares.



Esta vigilancia les permite comercializar su propia herramienta(Foto: Especial)

Tales sistemas comenzaron a aparecer en la región hace más de una década, incluso en 2007, cuando el alcalde de la Ciudad de México (ahora ministro de Relaciones Exteriores de México) Miguel Ebrard regresó de un viaje China con un acuerdo para instalar miles de cámaras chinas para combatir la delincuencia en la capital mexicana. Los ejemplos más recientes incluyen ECU-911 en Ecuador, un sistema nacional de vigilancia y comunicación creado inicialmente por China y acordado inicialmente por la administración antiestadounidense del presidente populista Rafael Correa. El sistema, que se ha extendido para incluir actualmente 4.300 cámaras y un centro de comando atendido por miles de ecuatorianos, se ha construido casi completamente con equipos chinos, diseñados para una variedad de propósitos nobles, desde respuestas de emergencia y combate al crimen, hasta monitoreo de volcanes. Bolivia cuenta con un sistema similar construido en China, aunque de alcance más limitado, BOL-110, además de cientos de cámaras de vigilancia donadas por China a al menos cuatro de sus principales ciudades.

En Panamá, que abandonó Taiwán para establecer relaciones con la República Popular China en 2017, el gobierno de Juan Carlos Varela acordó permitir que Huawei instale un sistema de cámaras en la ciudad de Colón y la zona de libre comercio asociada. No por casualidad, en julio de 2019, Hikivision, el mayor productor de cámaras de vigilancia de China, anunció planes para establecer un importante centro de distribución en Colón para dar soporte a las ventas de sus productos en todo el continente americano.



Tecnología de reconocimiento facial, capacidad de integrar datos de diferentes sensores. (Foto: Especial)

En el norte de Argentina, cerca de donde los chinos están desarrollando una operación de extracción de litio y construyendo el mayor despliegue de celdas fotovoltaicas del hemisferio para la generación de electricidad, la empresa china ZTE está instalando otro sistema de respuesta de emergencia de estilo "911" con 1.200 cámaras.

En Venezuela, aunque no es un sistema de vigilancia en sí mismo, la empresa china ZTE ha ayudado al régimen de Nicholas Maduro a implementar un "documento de identidad de la patria" que vincula diferentes tipos de datos sobre individuos a través de un documento de identidad que le permite al estado conferir privilegios (como racionamiento de alimentos) como herramienta de control social.

Al igual que con sectores como las computadoras y las telecomunicaciones, la República Popular China desea apoyar la exportación global de tales sistemas por parte de sus compañías para promover tecnologías que reconoce como estratégicas para la nación china, según sus propios documentos oficiales de política, como Made In China 2025.

Los riesgos derivados de la difusión del uso del equipo y las arquitecturas de vigilancia chinos son múltiples y significativos, e incluyen: 1. la sensibilidad de los datos recopilados sobre personas y actividades específicas, especialmente cuando se procesan a través de tecnologías como el reconocimiento facial, integrado con otros datos, y analizado a través de inteligencia artificial (AI) y otros algoritmos sofisticados; 2. la capacidad potencial para obtener subrepticiamente el acceso a esos datos, no solo a través de los dispositivos de recolección, sino en cualquier número de puntos a medida que se comunican, almacenan y analizan; y 3. el potencial a largo plazo para que dichos sistemas contribuyan al mantenimiento de regímenes autoritarios (como los de Venezuela, Bolivia, Cuba y anteriormente Ecuador) cuyas elites corruptas brindan acceso estratégico y beneficios comerciales al estado chino.

Uruguay tuvo relación en la última década con China para establecer una “Asociación estratégica”.(Foto: Especial)

El riesgo que plantean estas arquitecturas chinas se subestima simplemente al centrarse en las cámaras y los sensores.

Las tecnologías de reconocimiento facial y de otro tipo, y la capacidad de integrar datos de diferentes sensores y otras fuentes, como los teléfonos inteligentes, permiten a las personas con acceso a la tecnología seguir el movimiento de seres humanos y eventos individuales, con implicaciones alarmantes. Eso incluye la capacidad de trackear potencialmente a las elites políticas y empresariales, los disidentes u otras personas de interés, marcando posibles reuniones entre dos o más, y las implicaciones asociadas con las reuniones políticas o de negocios y los eventos que pueden producir. Los flujos de bienes u otras actividades alrededor de edificios gubernamentales, fábricas u otros sitios de interés pueden proporcionar otros tipos de información para obtener ventajas políticas o comerciales, desde ofertas ganadoras hasta chantaje a personas comprometidas.

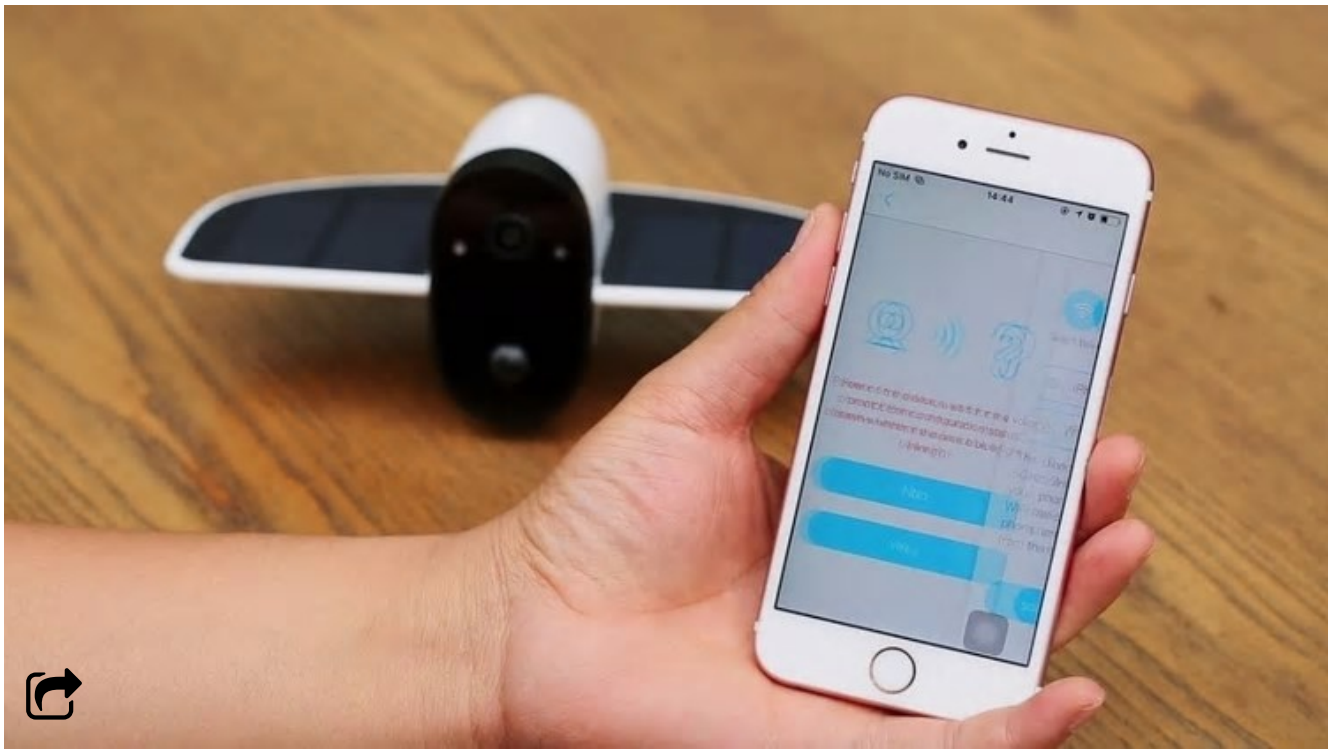
La cibervigilancia se ha extendido en los últimos años (Foto: Especial)

Si bien algunos pueden estar seguros de que las cámaras y otros componentes están protegidos de manera segura por gobiernos o compañías benévolas, la naturaleza dispersa de las arquitecturas, la información, las instrucciones y el análisis a través de grandes distancias, significa que el mayor riesgo no es el acceso físico a las cámaras, sino el desvío de información a lo largo del proceso, particularmente por aquellos que construyeron los componentes, bases de datos y sistemas de comunicación, y por aquellos que escribieron los algoritmos (cada vez más, chinos).

Con respecto al impacto político de tales sistemas, mientras que los gobiernos democráticos pueden instalarlos para propósitos nobles como la lucha contra el crimen y la respuesta ante emergencias, y con limitaciones que respetan la privacidad individual, los regímenes autoritarios que contratan a los chinos para implementar tales tecnologías no son tan limitados, y tienen todo los incentivos para usar la tecnología para combatir la disidencia y mantenerse en el poder.

La República Popular China, que continúa perfeccionándola contra su propia población en lugares como Xinjiang (contra los musulmanes uigures), no solo se beneficia comercialmente de la venta de la tecnología, sino que también se beneficia cuando las dictaduras aliadas proporcionan un campo de prueba para el desarrollo de productos y su uso para combatir a la oposición, mantener a amigos como Maduro en el poder, continuar entregando los bienes y el acceso a Beijing.

Al igual que en el debate sobre Huawei, ya sea que las empresas chinas estén explotando o no los sistemas de vigilancia y control que están implementando en América Latina para beneficiar al estado chino, la ley china (bajo la cual operan) requiere que lo hagan, si el gobierno de la República Popular China así lo exige.



Panamá utilizó Hikivision, cámaras chinas de vigilancia (Foto: Soliom)

El registro de espionaje sistemático, transferencia de tecnología forzada y otros malos comportamientos de China no debería dejar a nadie en América Latina tranquilo de que la China no aprovechará, en algún momento en el futuro, una oportunidad tan enorme.