# El nuevo juego de herramientas de los regímenes autocráticos

**La próxima generación de tecnología represiva hará que los esfuerzos pasados para difundir propaganda y anular la disidencia, parezcan primitivos**

Richard Fontaine y Kara Frederick 15 de marzo de 2019

Las autoridades chinas están utilizando ahora la herramienta del big data para detectar las desviaciones de un comportamiento "normal" entre los musulmanes de la región de Xinjiang... y a continuación identificar cada supuesta desviación para su posterior análisis por parte del estado. El gobierno egipcio planea trasladarse desde El Cairo a finales de este año a una nueva capital que tendrá, como dijo el portavoz del proyecto, "cámaras y sensores en todas partes, con un centro de mando para controlar toda la ciudad". Moscú ya tiene unas 5.000 cámaras instaladas con tecnología de reconocimiento facial y puede comparar los rostros de las personas que el estado tiene fichadas, con las fotos de las bases de datos de pasaportes, archivos de la policía e incluso de VK, la red social más popular.

Por muy distópicos y represivos que suenen estos métodos, sólo es el principio. Puede que pronto parezcan pintorescas tácticas de antaño. Un nuevo y sofisticado conjunto de herramientas tecnológicas - algunas de ellas ya están madurando, otras están listas para emerger en la próxima década- parecen destinadas a terminar en manos de los autócratas de todo el mundo. Permitirán a los hombres fuertes y a los estados policiales reforzar su dominación interna, socavar los derechos básicos y extender las prácticas antiliberales más allá de sus propias fronteras. China y Rusia están preparadas para aprovechar esta nueva gama de productos y capacidades, pero pronto estarán también disponibles para su exportación, para que incluso las tiranías de segundo nivel puedan controlar mejor y engañar a sus poblaciones.

Muchos de estos avances darán a los autócratas nuevas formas de difundir la propaganda, tanto interna como externamente. Una tecnología clave es la microsegmentación automática. Hoy en dio, la microsegmentación se basa en adaptar los contenidos a los segmentos de una población, en función de su psicología, características demográficas o de comportamiento. La Agencia de Investigación de Internet de Rusia realizó este tipo de investigación durante las elecciones en USA del año 2016 recolectando datos de Facebook para crear mensajes específicos para cada votante, basados en parte en la raza, etnia e identidad. Cuanto más potente sea la microsegmentación, más fácil será para las autocracias influir en la narrativa y el pensamiento.
Hasta ahora, esos esfuerzos se han limitado principalmente al mundo comercial y se han centrado en la publicidad de precisión: El propio Facebook lleva a cabo microsegmentación y Google etiquetó a los usuarios como "de tendencia a la izquierda" o "de tendencia a la derecha" para los anunciantes políticos en las elecciones de 2016.

Pero las empresas privadas están desarrollando inteligencia artificial que puede automatizar esta personalización para poblaciones enteras, y los gobiernos seguramente estará interesado. En octubre de 2018 en el Consejo de Relaciones Exteriores, Jason Matheny, ex director de Proyectos de Investigación Avanzada de Inteligencia del gobierno de los EE.UU. citó este tipo de "industrialización de la propaganda" como una razón para tener cuidado con la "exuberancia de IA en China y Rusia". Las aplicaciones impulsadas por la IA pronto permitirán a los autoritarios analizar los patrones en la actividad on line de la población, identificar a los más susceptibles a un determinado mensaje y apuntar a ellos con la propaganda de manera más precisa. En un TED Talk en 2017, el tecno-socialista Zeynep Tufekci describió un mundo donde "la gente en el poder utiliza estos algoritmos para observarnos ocultamente, juzgarnos y darnos un toque de atención, para predecir e identificar a los alborotadores y a los rebeldes". El resultado, sugiere, puede ser un autoritarismo que transforma nuestras pantallas privadas en "arquitecturas de persuasión a escala... para manipular a los individuos uno por uno, usando sus debilidades y vulnerabilidades personales individuales". Es probable que esto signifique unas "campañas de influencia" mucho más efectivas, dirigidas a los ciudadanos de países autoritarios o a los de democracias extranjeras. Las tecnologías

emergentes también cambiarán la forma en que los autócratas difunden propaganda. Los "bots" (cuentas automatizadas) on line controlados por el estado ya son una plaga en las redes sociales. Por ejemplo, durante la invasión de Crimea por parte de Rusia en 2014 y en los meses posteriores, los investigadores de la Universidad de Nueva York descubrieron que la mitad de los tweets de las cuentas que se centraban en la política rusa fueron generados por bots. El asesinato en octubre de 2018 del columnista del Washington Post, Jamal Khashoggi, provocó un aumento de mensajes de bots saudíes pro régimen.

Pero los bots pronto serán indistinguibles de los humanos on line, capaces de denunciar a los activistas anti-régimen, atacar a los rivales y amplificar el envío de mensajes oficiales de forma alarmantemente real. Lisa-Marie Neudert, una investigadora del Proyecto de Propaganda Computacional de Oxford, ha advertido que "la próxima generación de bots se está preparando para el ataque. Esta vez, los bots políticos dejarán las tareas repetitivas y automatizadas y se convertirán en inteligentes". Los avances técnicos que hacen funcionar a Alexa de Amazon y a Siri de Apple, dijo ante el Foro Internacional de Estudios Democráticos el pasado mes de octubre, también están enseñando a los bots de propaganda cómo hablar. Durante años, el gobierno chino ha empleado lo que se conoce como el "ejército de los 50 céntimos" - miles de falsos comentaristas pagados - para publicar mensajes on line favorables a Beijing y así ningunear las críticas que aparecen on line. En el futuro, los bots harán el trabajo de las actuales legiones de oficinistas pagados por el régimen.

Estos cada vez más insidiosos bots trabajarán junto con otras nuevas herramientas para que las dictaduras difundan desinformación, incluyendo "falsificaciones profundas"- falsificaciones digitales imposibles de distinguir del audio, video o imágenes auténticas.
Las falsificaciones de audio ya se están volviendo lo suficientemente buenas como para engañar a muchos oyentes: Sistemas de síntesis de voz hechos por compañías como Lyrebird (que dice que crea "las voces artificiales más realistas del mundo") tan solo requieren un minuto de grabación de la voz original para generar un audio aparentemente auténtico del orador elegido.
El vídeo está a punto de llegar. En YouTube, ya se puede ver uno de los actores Steve Buscemi y Jennifer Lawrence y otro video de baja calidad hecho por la compañía china iFlytek mostrando a Donald Trump y Barack Obama “hablando" en un mandarín fluido. Pronto, tales falsificaciones serán escalofriantemente convincentes.

Según el profesor de informática de Dartmouth, Hany Farid, "Probablemente hay de 100 a 1.000 veces más personas desarrollando tecnología para manipular contenidos que para detectar las manipulaciones. Llegaremos a afirmar que cualquier cosa es falsa. Y entonces ¿cómo vamos a creer en nada?"
Las nuevas herramientas también harán posible que los dictadores para llevar a cabo la vigilancia como nunca antes, tanto on line como en el mundo real. Los humanos están entrenando a computadoras para identificar e interpretar contexto emocional dentro de bloques de texto utilizando el procesamiento de lenguaje natural (una aplicación del software de ordenadores que aprenden). Facebook ahora utiliza técnicas similares para examinar los matices lingüísticos en los mensajes que podrían identificar a los usuarios que estén pensando en suicidarse. Empresas más pequeñas ya están trabajando para clasificar los posts en las redes sociales basados en la actitud, la emoción y la intención.

La empresa de inteligencia artificial Predictim, con sede en California, analizó los mensajes que las aspirantes a niñeras ponían en Twitter, Facebook e Instagram para clasificarlas por el nivel de riesgo potencial que representaban. Basándose únicamente en el lenguaje en los medios sociales de las potenciales niñeras, la aplicación proporcionó evaluaciones automáticas de su propensión para maltratar, ser irrespetuosas o usar drogas. La puesta en marcha del proyecto desencadenó un rápido rechazo el año pasado, pero China, Rusia y otras autocracias no compartirán tales escrúpulos. Jack Clark, que dirige la política de la empresa de investigación OpenAI, advierte que "actualmente no estamos, a nivel nacional o internacional, evaluando o midiendo el ritmo de progreso de las capacidades de la IA y la facilidad con la que determinadas capacidades pueden ser modificadas con fines maliciosos. Es como volar a ciegas en medio de un tornado: algo nos va a pasar..."

La próxima generación de herramientas de procesamiento de lenguaje natural será más sofisticada, a medida que se aceleran los avances en el aprendizaje de las máquinas. Aplicado por el régimen político equivocado, pueden combinarse con otros datos para evaluar la confianza, el patriotismo y la probabilidad de disentir.
Esas aplicaciones no existen todavía, pero un primer paso en esa dirección ya puede ser visto en las declaraciones públicas de China. Como ha informado The Wall Street Journal, "Para 2020, el gobierno chino espera implementar un sistema nacional de 'crédito social' que asignaría a cada ciudadano una calificación basada en cómo se comporta en el trabajo, en lugares públicos y en sus operaciones financieras". Los gobiernos regionales de China ya están manteniendo registros digitales del comportamiento de los ciudadanos y les están fichando por cruzar la calle imprudentemente, romper las reglas de planificación familiar o pagar sus deudas tarde. Aquellos que terminan en la lista negra son castigados: no pueden comprar billetes de tren de alta velocidad, obtener subsidios del gobierno, comprar bienes raíces o incluso conseguir un trabajo. De acuerdo con un plan emitido por el gobierno municipal de Beijing, para el 2021, los ciudadanos de la lista negra de la capital serán "incapaces de moverse ni un solo paso".
Venezuela ha introducido su propio "carnet de la patria", un carnet basado en un chip inteligente que los ciudadanos necesitan para tener acceso a servicios públicos como la atención sanitaria y los alimentos subvencionados. La ONG Human Rights Watch informa que ese carnet puede registrar también el historial de votación del ciudadano. Los datos que este sistema genera son almacenados por la empresa china ZTE, que también ha desplegado un equipo de expertos dentro de la compañía nacional de telecomunicaciones de Venezuela, Cantv, para ayudar a poner en marcha el proyecto, según una Investigación de Reuters en 2018. Yoshua Bengio, un informático conocido como uno de los tres "padres" del aprendizaje profundo en la IA, recientemente describió a Bloomberg sus preocupaciones sobre el creciente uso de la tecnología para el control político. "Este es el escenario del "Gran Hermano", dijo, "creo que cada vez da más miedo".

La capacidad de los autócratas para espiar a sus ciudadanos será mejorada por los avances en la inteligencia artificial que sacan partido de las enormes bases de datos (Big Data). Tanto en EE.UU. como en China, las empresas están optimizando nuevos chips que incluyan redes neuronales - un algoritmo inspirado en cómo funciona el cerebro humano. El Ministerio de Industria y Tecnologías de la Información de China recientemente dijo que en 2020 esperaba producir en masa chips de red neuronal.

Permitirán a los regímenes opresivos reunir más eficazmente información sobre las conversaciones y el comportamiento de su población, examinar los conjuntos de datos masivos y explotar rápidamente la información. Una aplicación particular de la IA, el reconocimiento facial, podría estar tan extendida en una década como lo son hoy las cámaras de los smartphones. La tecnología ha sido utilizada por el Departamento de Seguridad Nacional de EE.UU., la policía de San Diego y otros para mejorar la seguridad en grandes eventos como la Super Bowl de football. En las manos de los autócratas, sin embargo, la tecnología tiene un gran potencial para uso represivo. La policía china desplegó gafas de reconocimiento facial a principios 2018, y la empresa LLVision Technology Co. con sede en Beijing vende versiones básicas a países de África y Europa. Estas gafas pueden utilizarse para ayudar a identificar criminales como ladrones y traficantes de drogas, o para cazar activistas de derechos humanos y manifestantes pro-democracia. Un disidente político en Harare pronto puede tener tanto que temer como un traficante de heroína en Zhengzhou: La empresa china de inteligencia artificial CloudWalk Technology ha vendido al gobierno de Zimbabwe un sistema de reconocimiento facial masivo que recogerá en masa información de reconocimiento facial de los ciudadanos de Zimbabwe y la enviará a la compañía en China; allí se depurarán los datos y se mejorará el algoritmo para hacer más eficaz el sistema.

El negocio está también en auge para otras empresas. La lista de clientes globales de la empresa china de videovigilancia Tandy, que fabrica sistemas inteligentes de seguridad, incluye a más de 60 países.  La aparición de nuevas "ciudades inteligentes" en todo el mundo también podría significar problemas. Los regímenes autocráticos podrán combinar datos de diversas fuentes para tejer una red de control social. China planea construir ciudades más inteligentes como Yinchuan, donde los viajeros pueden usar una identificación facial positiva para subir a un autobús, o Hangzhou, donde los datos faciales pueden ser usados para comprar una comida en KFC. Las megalópolis planificadas como la nueva área de Xiong'an, al suroeste de Beijing, sugiere la forma que tendrán los futuros "grandes ojos que todo lo ven". Estas ciudades del futuro podrían utilizar sistemas centralizados de control usando los registros financieros, penales y gubernamentales, basándose en sitios web, imágenes visuales, aplicaciones telefónicas y sensores, todo ello impulsado por la transmisión de datos 5G.


Hasta hace poco, era fácil ver la revolución digital como un gran liberador, una forma de transmitir ideas más rápido que cualquier posible censor. La realidad está resultando ser mucho más complicada. Internet hizo ampliamente disponibles los datos, pero los nuevos avances tecnológicos pueden concentrar el poder de los datos en las manos de unos pocos. Con más de 30 mil millones de dispositivos que se espera que se conecten a Internet para el 2020, cada uno generando nuevos datos, aquellos que puedan controlar, procesar y explotar esa cantidad inmensa de información tendrán un gran ventaja. Un régimen empeñado en auto-perpetuarse puede sentirse virtualmente obligado a hacerlo.

Pero no debemos asumir que las ventajas serán solo para los gobiernos opresivos. Cuando las dictaduras buscaron en los últimos años controlar las comunicaciones on line de sus ciudadanos, el Departamento de Estado de EE.UU. y otros patrocinaron herramientas de encriptación que permitieron a los posibles disidentes comunicarse de forma segura. Cuando los regímenes censuraron la información y bloquearon el acceso a sitios web importantes, surgieron herramientas para permitir un acceso sin restricciones. Esa es la idea correcta. Las sociedades abiertas necesitarán generar una serie de respuestas para la confrontación que se avecina. Las democracias necesitarán aplicar sanciones a los individuos y grupos que usen las nuevas herramientas para fines represivos, sancionar a las empresas tecnológicas que hayan sido cómplices de abusos de los derechos humanos, invertir en contramedidas y endurecer sus propios sistemas contra las intrusiones externas. Los gobiernos libres también tendrán que diferenciar entre usar las nuevas tecnologías para fines legítimos (como hacer cumplir la ley) o bien utilizarlos para consolidar el control partidista, reducir los derechos ciudadanos  o inmiscuirse en las democracias de otros países.

Los dictadores, desde Caracas a Pyongyang, tratarán de explotar el enorme potencial inherente a las tecnologías emergentes para el mal uso político, así como han hecho durante décadas con la radio, la televisión y la propia Internet.
Las democracias necesitarán estar preparadas para luchar.

El Sr. Fontaine es el CEO del Centro para una Nueva Seguridad Americana en Washington, D.C.
La Sra. Frederick es una asociada del centro y programa de seguridad y trabajó anteriormente para Facebook, el Comando de Guerra Especial de la Marina de los Estados Unidos y el Departamento de Defensa.